Paybox

PAYBOX SYSTEM

INTEGRATION MANUAL

VERSION 6.2

05/06/2014

VeriFone®
THE WAY TO PAY™

CHANGE REVIEW

DATE	VERSION	DESCRIPTION	AUTHOR
12/07/2012	5.09	Initial English version after refactoring Document dedicated for Paybox System	Projects Team
20/07/2012	5.10	§11.3.7 PBX_ONEY_DATA tags cannot be translated	Projects Team
02/09/2013	6.00	BCMC integration New variables : PBX_ATTENTE, PBX_NBCARTESKDO, PBX_CK_ONLY, PBX_GROUPE Payment selection page customization	Projects Team
27/11/2013	6.1		Projects Team
05/06/2014	6.2	New corporate identity and style guide	Projects Team

REFERENCES DOCUMENTATIONS

Most of the documents below are available on the Paybox Web site for download www.paybox.com :

REF.	DOCUMENT	DESCRIPTION
Ref 1	ManuelIntegrationPayboxDirect_V6.2_EN.pdf	Integration manual of the Paybox Direct / Direct+ solution
Ref 2	ParametresTestPaybox_V6.1_EN.pdf	Document describing test parameters and preproduction environment.
Ref 3	GUIDE_UTILISATEUR_BACK_OFFICE_COMMERCANT_PAYBOX.doc	User guide for Merchant Back Office
Ref 4	PAYBOX Fiche présentation 3DSecure.pdf	Introduction to 3-D Secure : advantages for the merchant and FAQ
Ref 5	Paybox manuel en français V4_84.pdf	Integration guide for the previous version of Paybox System with CGI module
Ref 6	Paybox System - Personnalisation de la page et ticket de paiement.pdf	Integration guide for the personalization of the payment page
Ref 7	NoteTechniqueIntégration_PageChoixPayboxSystem_V1.21.pdf	Integration note to customize the payment type selection page
Ref 8	Note Paypal	Integration note for Paypal
Ref 9	Note Kwixo	Integration note for Kwixo
Ref 10	Note Oney	Integration note for Oney

WARNING

This document is the property of Paybox/Point Transaction Systems. Any copy, partial or complete, any disclosure or use by third parties is strictly forbidden without express written consent from Paybox/Point Transaction Systems.

If you discover some errors in this documentation, you can send us an e-mail (see e-mail addresses below) describing the error or the problem as precisely as possible. Please provide in your e-mail the document reference and the page number.

INFORMATION

For any Merchant or Integrator who needs some commercial information, Paybox Sales team is available from Monday to Friday, from 9 am to 6 pm:

Sales department:

e-mail: contact@paybox.com

Phone: + 33 (0)1 61 37 05 70

SUPPORT

For any Merchant or Integrator who needs some technical information or support during the integration process, Paybox Support team is available from Monday to Friday, from 9 am to 12.30 pm and from 2 pm to 6.30 pm (5.30 on Friday) :

Technical & Functional Support:

e-mail: support@paybox.com

Phone: + 33 (0)4 68 85 79 90

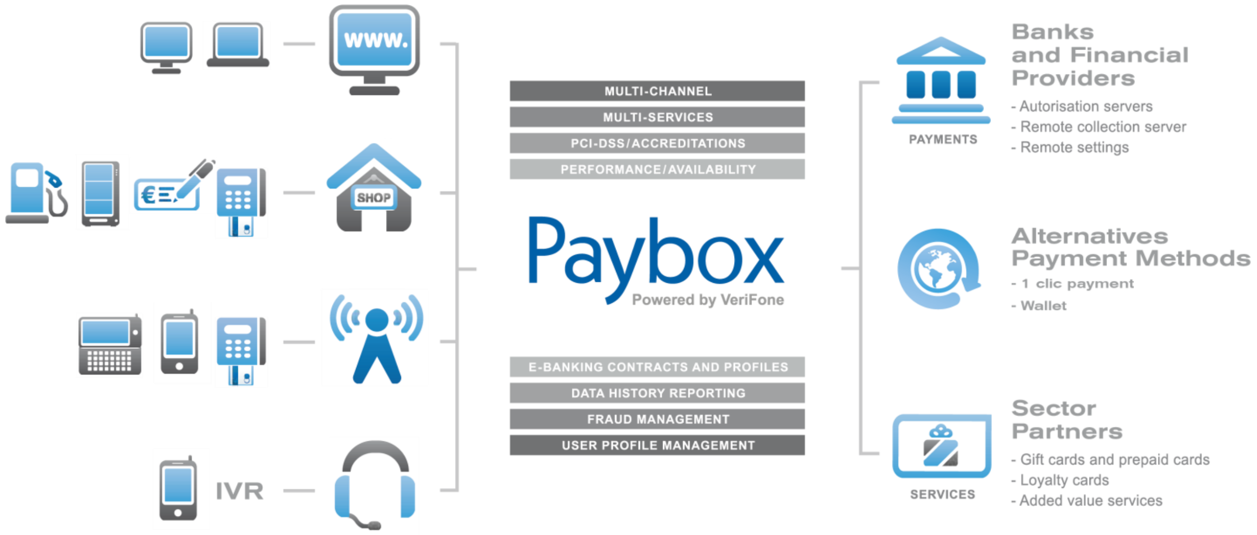
For any contact with our Sales or Support teams, you MUST provide the following PAYBOX identifiers:

- SITE number (7 digits)
- RANG number (2 digits)
- IDENTIFIANT number (1 to 9 digits)

TABLE OF CONTENTS

1. INTRODUCTION

Paybox / Point Transaction Systems has developed and is managing its own centralized platform to provide an interface between different channels for payments or services and the corresponding recipients for processing (financial operators, banking institutions, business partners).



It is a multi-channel and multi-services centralized platform:

➢ Multi-channel : the PAYBOX platform accepts connections originating from different kind of systems, physical POS (Card Present) as well as remote payments (Card Not Present, E-Commerce/M-Commerce) :
- Internet, Merchant Web Sites
- Electronic Payment Terminals, POS in a shop or retailer
- Vending machines
- Smartphones or PDA
- Call centers, Interactive vocal servers (IVR), …

➢ Multi-services : the PAYBOX platform is able to process many different types of payments instruments:
- Debit cards and credit cards,
- Private label cards,
- Gift cards,

But the platform is also able to process multiple services and business oriented transactions :
- Loyalty cards,
- Consumer finance,
- Fleet management,
- Taxi booking, …

2. PURPOSE OF THIS DOCUMENT

In the Card Not Present and E-Commerce/M-Commerce areas, Paybox is offering several solutions, each of them offering specific functionalities:

- **PAYBOX SYSTEM**: PAYBOX SYSTEM is an integration with the Merchant Web or mobile site. At the time of payment, cardholders are automatically redirected to a secured multi-lingual payment page hosted by PAYBOX. This payment page can be personalized to fit the Merchant Web Site look and feel. PAYBOX SYSTEM complies with the highest security requirements for card payments on E-Commerce/M-Commerce Web Sites by using amongst others, an SSL 256 bits technology for the payment page and by managing the 3-D Secure protocol (if option subscribed by the Merchant).

- **PAYBOX DIRECT (PPPS)**: PAYBOX DIRECT ensures processing of payment in the most seamless way for the cardholder who will not be redirected. The merchant sales application has to collect the card information (such as Card number, expiry date …) and send it to PAYBOX within a SSL secure server to server request, in order to process the payment.

  Paybox Direct can also be used to capture transactions which have already been authorized through PAYBOX SYSTEM. Combining Paybox System with Paybox Direct allows merchants to improve flexibility by driving their operations post-payment in server to server mode, directly from their sales application (or back-office).

- **PAYBOX DIRECT *Plus***: Refers to the Paybox service where the sales application asks Paybox to store cardholder information. This solution interfaces nicely with Paybox System or can be used alone directly in server to server mode.
  Paybox Version Plus allows the merchant to manage recurring payments, as well as express checkouts with 1-click payment where the cardholder doesn't have to enter its data for each transaction.

- **PAYBOX BATCH FILE PROCESSING**: This solution is based on mutual off-line deposits of structured files between the merchant and Paybox. The merchant information system has to collect the card information (such as Card number, expiry date …) and send it to PAYBOX through a secure file transfer, in order to process the payments. PAYBOX BATCH FILE PROCESSING can also be used to capture transactions which have already been authorized through PAYBOX SYSTEM. PAYBOX BATCH FILE PROCESSING also provides functionalities like refund and cancel of transactions, again through file deposit mechanism.

This document is the integration manual for the **PAYBOX SYSTEM** solution.

It is intended to people who need some information on the PAYBOX SYSTEM solution, its behavior, functionalities, interface and the best practices for integration.

3. INTRODUCTION TO THE « PAYBOX SYSTEM » SOLUTION

3.1 General overview

« Paybox System » is a secure solution for processing payments by bank cards, credit cards or other payment means for payments on Merchant Web Sites.

For the « Paybox System » integration, there is no module to install, neither on the Merchant Web site, nor on the computer of the cardholder who wants to pay.

Once the solution has been integrated with the Merchant Web site, the cardholder can pay in a total secure manner: when his order is completed, he is redirected to the PAYBOX platform which will create an encrypted connection with the cardholder (using SSL 256 bits technology which guarantees that the confidential card information will be protected during transport) and display the PAYBOX payment page within which the cardholder can safely enter his card information.

Paybox System will then control the validity of the card information by sending an authorization request to the acquiring server associated to the payment instrument used, in compliance with the current standards and security rules for payments processing.
If the payment is accepted, a receipt is then displayed on the screen of the cardholder (option). He will also receive this receipt by e-mail as a proof which confirms the payment.
The cardholder may then go back to the merchant web site to continue his shopping.

Paybox System will also send by e-mail to the merchant a copy of the payment receipt. The merchant will be able to automatically process the result of the payment by analyzing the various information elements returned by Paybox System.

At the end of the day, Paybox System will gather all the payments accepted on the Merchant Web site during the day and will send them to the collecting center of the acquirer for processing.

Once the collection process is finished, the Merchant will receive by e-mail a receipt describing the result and detailed information of the collect.

3.2 List of payment methods

Below is a list of all payment methods supported by Paybox:

PAYMENT METHOD	TYPE	COMMENT
CB, VISA, MASTERCARD	Credit card	
MAESTRO	Debit card	3-D Secure mandatory
BANCONTACT MISTERCASH	Debit card	Belgian card 3-D Secure mandatory
E-CARTE BLEUE	Dynamic virtual Credit card	Processed by VISA France
AMERICAN EXPRESS	Credit card	
JCB	Credit card	
DINERS	Credit card	
COFINOGA	Credit revolving card	
SOFINCO	Credit revolving card	
FINAREF	Credit revolving card	Cards SURCOUF, KANGOUROU, FNAC, CYRILLUS, PRINTEMPS, CONFORAMA
CETELEM / AURORE	Credit revolving card	
AVANTAGES		Card Casino Avantages
CDGP	Credit revolving card	Card Cofinoga Quelle
RIVE GAUCHE		
PAYSAFECARD	Prepaid card	
WEXPAY	Prepaid card	Non reloadable
KADEOS	Prepaid gift card	
SVS	Prepaid gift card	Gist card Castorama and Etam
LASER	Prepaid gift card	Gift card
1EURO.COM	On-line loan	
PAYPAL		Requires an account at Paypal
BUYSTER	Payment via mobile	
KWIXO	C2B payment and C2C transfer	
LEETCHI	Online pot	
MAXICHEQUE	Gift checks	

ONEY	Online prepaid card Online funding	
PAYBUTTON ING	On-line account to account payment	Requires a merchant bank account at ING Belgium
iDEAL	On-line account to account payment	Requires a merchant bank account at ABN AMRO, RABOBANK or ING NL

3.3 Security

3.3.1 Identification

A Merchant Web site is referenced within Paybox platform using different information fields:

- Site number (field SITE)
- Rank number (field RANG)
- An identifier (field IDENTIFIANT)

These identification parameters are provided by Paybox when the registration of the Merchant at PAYBOX is confirmed.

The merchant shall include these identification parameters into every request sent from his Web Site to PAYBOX platform for payments or any other transactions.

Furthermore, the merchant shall provide that information in every contact with the Sales team or the Support team.

3.3.2 Authentication

In order to guarantee the maximum security for the payments processed from the Merchant Web Site, all the requests sent from the merchant Web Site to PAYBOX platform are authenticated by a shared secret key, known only by the merchant and by PAYBOX.

This key will be used to seal every request sent by the Merchant Web site allowing PAYBOX to authenticate the origin of the request.

The merchant has to generate this key through his access to the PAYBOX Back Office and the chapter ***§8.2 Management of the HMAC authentication key*** in this document describes this procedure.

3.4 Introduction to the Paybox System pages

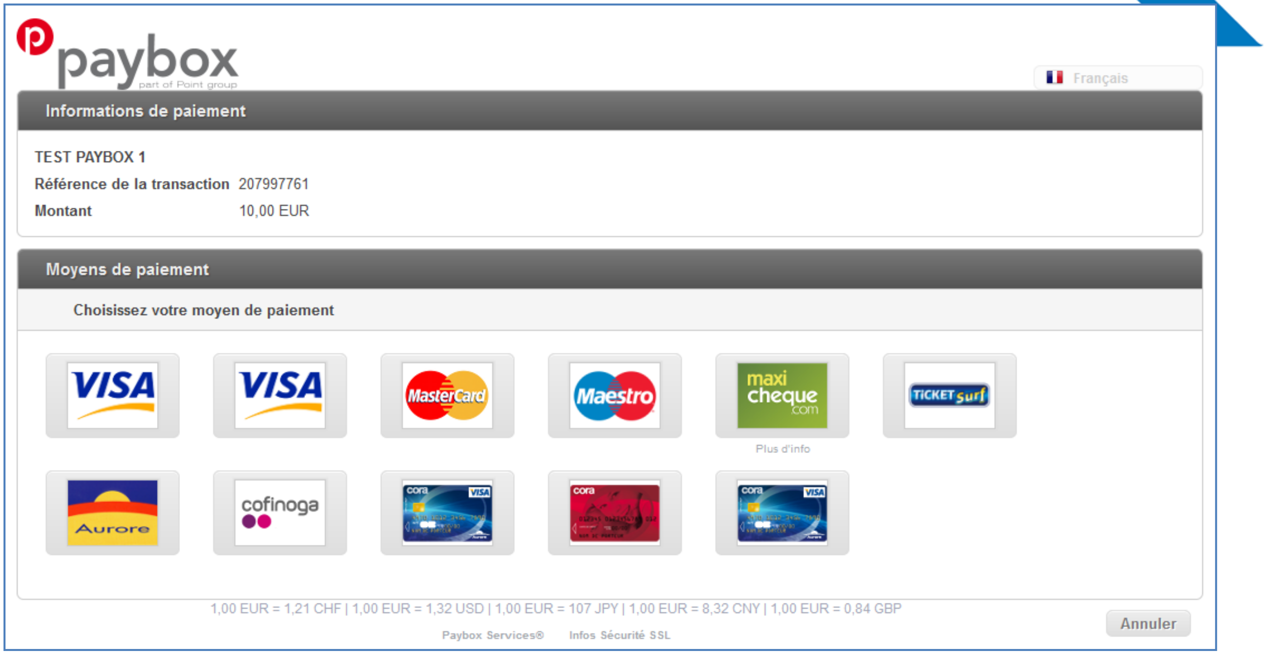
All along the payment process, different payment pages will be displayed:

3.4.1 Payment type selection page

This is the first page of the payment process and will be proposed to the customer (shopper) all the payment means supported by the merchant. Each customer is required to select a payment method. After the selection of the payment method a second page is shown that contains specific details related to the chosen payment method.

For example, the cryptogram CVC2 will not be asked for a Diners card but will be mandatory for an American Express or Visa or Mastercard payment.

Below is an example of how a payment method selection page looks like:



Informations de paiement

TEST PAYBOX 1

Référence de la transaction	207997761
Montant	10,00 EUR

Moyens de paiement

Choisissez votre moyen de paiement

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

Picture 1 : Page for payment mean selection (can be avoided)

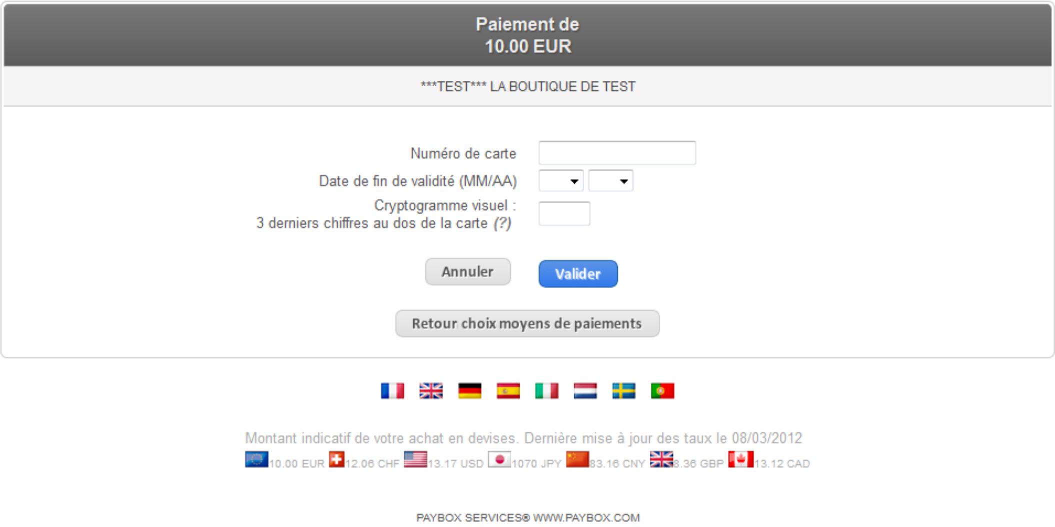
This page is not relevant if there is only one payment method to be chosen. As a result this page will not be displayed in case the merchant did not subscribe for more than one payment method. In that case the customer will automatically be redirected to the payment page.

- PAYBOX suggests that the payment method selection is done on the web site of the merchant. This is done by adding the logos of the different payment methods as clickable icons for every payment method. The cardholder will be redirected to the corresponding Paybox payment page for completing the payment process.

- For more information on handling different card types and payment methods, see chapter ***§4.2 Forcing payment type and payment mean*.**

This selection page can be customized. The customization options are described in a special integration note ***[Ref 7].***

3.4.2 Payment Page



Paiement de
10.00 EUR

TEST LA BOUTIQUE DE TEST

Numéro de carte

Date de fin de validité (MM/AA)

Cryptogramme visuel :
3 derniers chiffres au dos de la carte *(?)*

Montant indicatif de votre achat en devises. Dernière mise à jour des taux le 08/03/2012
10.00 EUR 12.06 CHF 13.17 USD 1070 JPY 83.16 CNY 8.36 GBP 13.12 CAD

PAYBOX SERVICES® WWW.PAYBOX.COM

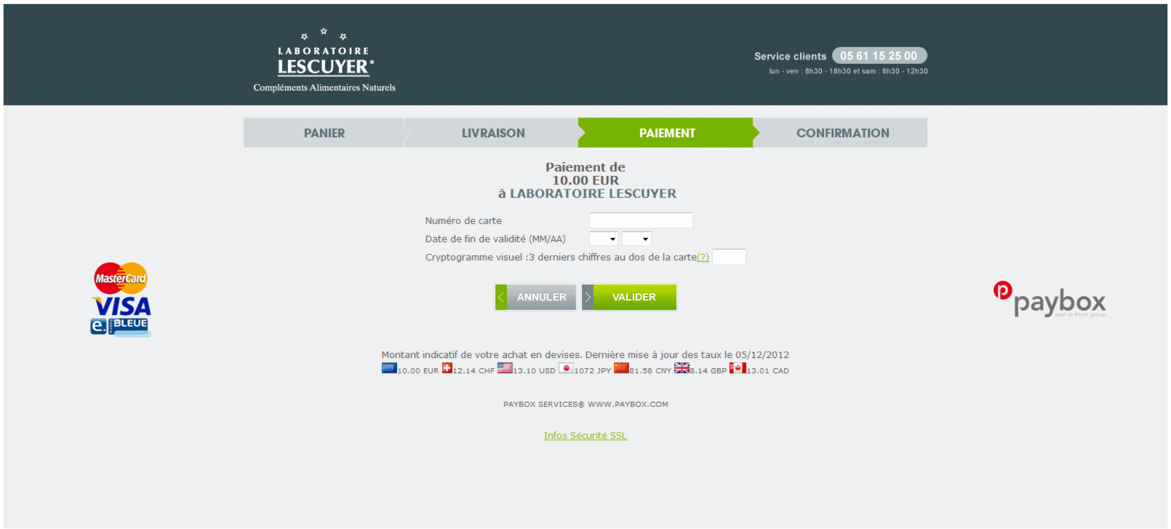
Picture 2 : Customizable payment page

The page displayed above is an example of a payment page personalized by a merchant. In order to increase the cardholder’s confidence during the payment process and to provide a better quality rendering, it is possible to personalize a lot of elements so that the page continues in the look and feel of the merchant’s web site.

The elements which can be personalized are:

- Logo on top of the page
- Display of the Paybox logo
- Design of the buttons : validate / cancel / back to shop
- Languages
- Background
- And many other options in a CSS file

To discover how to configure those different elements, please refer to the document ***[Ref 6] PAYBOX SYSTEM - Personalization of the page and payment receipt*.**



LABORATOIRE
LESCUYER®
Compléments Alimentaires Naturels
Service clients 05 61 15 25 00
lun - ven : 8h30 - 18h30 et sam : 8h30 - 12h30
PANIER
LIVRAISON
PAIEMENT
CONFIRMATION
MasterCard
VISA
e. BLEUE
paybox
ANNULER
VALIDER

Paiement de
10.00 EUR
à LABORATOIRE LESCUYER

Numéro de carte

Date de fin de validité (MM/AA)

Cryptogramme visuel :3 derniers chiffres au dos de la carte(?)

Montant indicatif de votre achat en devises. Dernière mise à jour des taux le 05/12/2012
10.00 EUR 12.14 CHF 13.10 USD 1072 JPY 81.58 CNY 8.14 GBP 13.01 CAD

PAYBOX SERVICES® WWW.PAYBOX.COM

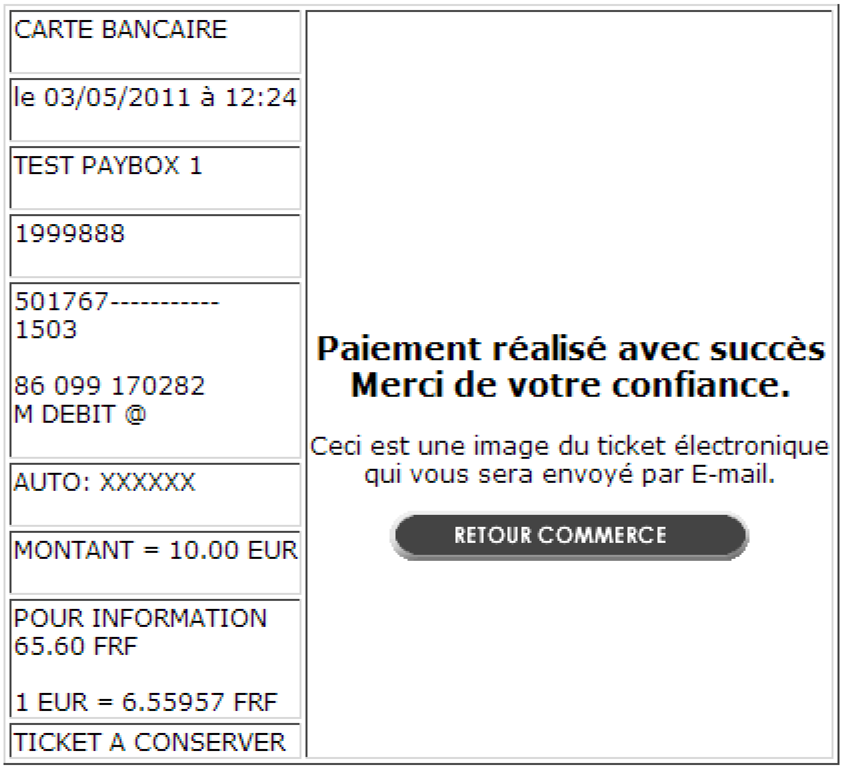
Infos Sécurité SSL

Picture 3 : Another example of personalization

3.4.3 Payment receipt

After the payment is successfully authorized, both the cardholder and the merchant receive by e-mail a payment receipt (exactly as on a physical terminal) starting with the 50 first characters from the order reference. The customer's email address will also be printed at the end of the receipt.

The customer will also be redirected to a page which confirms that the payment was successful. This page looks similar to the picture below:



CARTE BANCAIRE

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

Paiement réalisé avec succès
Merci de votre confiance.

Ceci est une image du ticket électronique
qui vous sera envoyé par E-mail.

Picture 4 : Confirmation page for a successful payment

- It is also possible to avoid this page and redirect, altogether with the payment results (rejection code or authorization number), the cardholder directly to the Merchant Web Site. See ***§5 Response management***.

- In the same way as on the payment page, it is possible to personalize the payment receipt that will be sent to the cardholder after the payment has been completed. For instance, it is possible to add a logo and a specific text.

- For more information on the possibilities, please refer to the document ***[Ref 6] PAYBOX SYSTEM - Personalization of the page and payment receipt***.

4. CALLING THE PAYMENT PAGE

In order to display the payment page to the customer who wishes to pay on the merchant web site, it is necessary to send to the Paybox System URL a HTTPS request with a list of parameters.

4.1 Construction of the request

The following parameters are mandatory in any request:

- PBX_SITE = Site number (provided by Paybox)
- PBX_RANG = Rank number (provided by Paybox)
- PBX_IDENTIFIANT = Internal identifier (provided by Paybox)
- PBX_TOTAL = Transaction amount
- PBX_DEVISE = Transaction currency
- PBX_CMD = Merchant reference for the order
- PBX_PORTEUR = E-mail address of the end customer
- PBX_RETOUR = List of parameters that Paybox should send back after the payment
- PBX_HASH = Type of hash algorithm used to calculate the HMAC hash
- PBX_TIME = Timestamp of the transaction
- PBX_HMAC = HMAC hash calculated with the secret key

The meaning of the mandatory and optional parameters is described later in this chapter*.*

All those parameters must be sent with the POST method to our payment platform.

To send over those parameters, it is possible to use this kind of form (given as an example):

```
<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="Send">
</form>
```

In this case, the only visible element on the page will be a button « Send ». When the customer will click on it, he will be automatically redirected to the Paybox System payment page.

The payment will be of 1000 Euros cents (10 Euros) and the unique link between the payment and the merchant order will be done through the reference « TEST Paybox ».
Once the payment is completed, if it is successful, an email containing a payment receipt will be sent to

the merchant as well as to the customer (shopper) by using the email address specified in the form (here « test@paybox.com »).
The merchant used in this test (site 1999888, rank 32 and identifier 2) is available for tests on Paybox pre-production platform.

More information concerning the test conditions on Paybox pre-production environment is available at chapter ***§10 Test Environment.***

Please note that the URLs used in the above example are dummy URLs.
Real URLs for production purpose are defined in chapter ***§12.6 URLs to call and IP addresses*****.**

4.2 Forcing payment type and payment mean

If the merchant prefers to manage on his web site the choice of payment instrument, it is possible to provide this information in the call to Paybox System payment page using the PBX_TYPEPAIEMENT and PBX_TYPECARTE parameters.

In this case, the customer will be directly redirected to the payment page specifically designed for the chosen payment method.

Example: For a payment with a CB card, PBX_TYPEPAIEMENT should be filled with « CARTE » and PBX_TYPECARTE with « CB ».

The list of possible values for those parameters is available in the chapter ***§11 Data dictionary***.

NOTE: the 2 parameters PBX_TYPEPAIEMENT and PBX_TYPECARTE should be used in combination. Using only one of both fields or filling them with unauthorized values would lead to problems for accessing the payment page or unexpected behavior during the payment phase.

4.3 Message authentication with HMAC hash

In order to secure the payment, i.e. make sure that the payments requests are really issued by the merchant and are not modified in any unauthorized way, Paybox requires to authenticate requests with a HMAC hash.

- Step 0: The merchant must generate a secret key via a dedicated menu available through his access to the Back Office. Process is described in the chapter ***§8.2 Management of the HMAC authentication key***.

- Step 1: when creating messages that will be sent to the Paybox servers, all parameters should be concatenated and separated with the « & » symbol. For the above message (§4.1), the result string should look like :

```
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_RETOUR= Mt:M;Ref:R;Auto:A;Erreur:E
&PBX_HASH=SHA512&PBX_TIME=2011-02-28T11:01:50+01:00
```

- Step 2: it is then possible to calculate the HMAC hash using :
  - The above result string
  - The secret key generated through the Back Office
  - The chosen algorithm (cf. PBX_HASH in ***§11 Data dictionary***)
- Step 3: the parameter PBX_HMAC in the request must then be filled with the result hash.

- The order of the parameters in the string used for hash calculation must be exactly identical to the order of the fields in the form (the request sent)
- In the string to be hashed, the data filled should be « rough », i.e. do not use URL encoding functions

Here is an example using PHP source code allowing to calculate the HMAC hash :

```
<?php
// Get the date at ISO-8601 format
$dateTime = date("c");
// Create the string to be hashed, without URLencoding
$msg = "PBX_SITE=1999888".
"&PBX_RANG=32".
"&PBX_IDENTIFIANT=2".
"&PBX_TOTAL=".$_POST['montant'].
"&PBX_DEVISE=978".
"&PBX_CMD=".$_POST['ref'].
"&PBX_PORTEUR=".$_POST['email'].
"&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E".
"&PBX_HASH=SHA512".
"&PBX_TIME=".$dateTime;


// Get the secret HMAC key (stored in a database for instance) and put it into $keyTest;

// If the key is in ASCII format, convert it to binary
$binKey = pack("H*", $keyTest);

// Calculate the HMAC hash (to be filled into parameter PBX_HMAC) with function hash_hmac and
// the binary key
// Send in the parameter PBX_HASH the hash algorithm which has been used (SHA512 in this case)
// To display the list of algorithms available on your environment, uncomment the following command
// print_r(hash_algos());

$hmac = strtoupper(hash_hmac('sha512', $msg, $binKey));
// The string will be sent in capital letters, so we use strtoupper()

// Create the HTML sheet that will be sent to Paybox System
// NOTE : the sequence of parameters in the request is extremly important, it must fit
// the sequnce of parameters in the hashed string
?>
<form method="POST" action="https://urlserveur.paybox.com/cgi/MYchoix_pagepaiement.cgi">
<input type="hidden" name="PBX_SITE" value="1999888">
<input type="hidden" name="PBX_RANG" value="32">
<input type="hidden" name="PBX_IDENTIFIANT" value="2">
<input type="hidden" name="PBX_TOTAL" value="<? echo $_POST['montant']; ?>">
<input type="hidden" name="PBX_DEVISE" value="978">
<input type="hidden" name="PBX_CMD" value="<? echo $_POST['ref']; ?>">
<input type="hidden" name="PBX_PORTEUR" value="<? echo $_POST['email']; ?>">
<input type="hidden" name="PBX_RETOUR" value="Mt:M;Ref:R;Auto:A;Erreur:E">
<input type="hidden" name="PBX_HASH" value="SHA512">
<input type="hidden" name="PBX_TIME" value="<? echo $dateTime; ?>">
<input type="hidden" name="PBX_HMAC" value="<? echo $hmac; ?>">
<input type="submit" value="Send">
</form>
```

If the merchant is already using the previous method to interface with Paybox System (with CGI module), the first call with the HMAC authentication method will block any future calls issued from the CGI interface.

4.4 Called URL

The list of available URLs for calling the Paybox servers is detailed in the chapter ***§12.6 URLs to call and IP addresses***.

In case the main URL is not available, backup URLs can be used. It is the responsibility of the merchant to make sure that the URL is available for processing before redirecting the customer.

It is possible to test the availability of the servers by trying to load an HTML page « load.htm ». This page only contains the string « OK » which confirms that the server is available for processing transactions.

Hereunder is an example of PHP source code allowing to test the availability of the URLs (Note that the URLs used in the example are dummy URLs and have to be replaced by the production URLs) :

```
<?php
        $servers = array('urlserver.paybox.com', // primary URL
                              'urlserver1.paybox.com'); // backup URL

        $serverOK = "";
        foreach($servers as $server){
                $doc = new DOMDocument();
                $doc->loadHTMLFile('https://'.$server.'/load.html');

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

                if($server_status == "OK"){
                        // Server is up and services are available
                        $serverOK = $server;
                        break;
                }
                // else : Server is up but services are not available .
        }


        if(!$serverOK){
                die("Error : no server found");
        }
?>

        //echo 'Connecting to https://'.$server.'/cgi/MYchoix_pagepaiement.cgi';
```

5. RESPONSE MANAGEMENT

Once the payment is completed, the customer may be redirected to the merchant web site, using one of 4 URLs.

The merchant is able to automatically manage order validation, depending on the result of the payment, by using a 5th URL called IPN (Instant Payment Notification).

5.1 Customer redirection

Depending on the payment outcome: accepted, rejected, cancelled or waiting confirmation, the redirection of the customer back to the merchant web site can use 4 different URLs:

- The URLs can be configured for every transaction through a parameter,
    - It allows redirecting every customer to a specifically personalized page.
    - The URLs must be configured for every transaction by correctly setting the following parameters : PBX_EFFECTUE, PBX_REFUSE, PBX_ANNULE, PBX_ATTENTE
- Either by using the predefined values stored in the merchant profile defined during registration
    - Those values have to be provided by the merchant during administrative registration process. Those predefined values can also be changed by the merchant through the « Information » menu in the Back Office interface.

The customer will be redirected to one of those pages after clicking on the button « back to shop » on the summary page after payment (when the payment receipt is displayed), or on the page explaining that the payment was not authorized.

It is also possible for the merchant to choose an automatic redirection: this option has to be defined during the administrative registration process or with the Helpdesk team. In that case, the payment receipt is not displayed and the customer is directly redirected to the merchant web site.

❗ It is strongly recommended not to use the parameter « PBX_EFFECTUE » to validate orders on the web site : this parameter is not secured and there is no guarantee that the redirection to the merchant web site will systematically work. Indeed, when the payment is finished, some customers may cut the connection and thus they will not be redirected to the merchant web site. For more details, see chapter ***§5.3 Orders Validation***.

❗ Those 5 parameters are URLs. In case they contain special HTML characters, they must be « URL Encoded » before to send them, it means to convert them to a specific character value compliant with encoding of URLs.
For instance, if the URL « PBX_EFFECTUE » contains character « ; », this character has to be replaced by « %3B » :

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

The parameter « PBX_EFFECTUE » should be filled as follows:

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

This restriction is called URL Encoding and is due to the management of the tag META HTTP-EQUIV in Internet Explorer.

Within the Annexes at the end of this document a list of the most frequent special characters and the corresponding value after « URL Encoding » is available.

5.2 Payments waiting confirmation

Some payment methods (examples: Paypal, iDeal…) can sometimes require a delay between a few hours and a few days before confirming the payment.

To inform you of the situation, Paybox sends a first response as soon as the client has finished his payment process, with the response code 99999 on the URL PBX_ATTENTE and via the IPN.

Paybox will then update the transaction status, and when the confirmation is done, Paybox calls back the merchant website via the IPN with the final response (ex: 00000 if the transaction is authorized).

For more information about those payment methods, please refer to the documents below :

- ***[Ref 8] Note Paypal***
- ***[Ref 9] Note Kwixo***
- ***[Ref 10] Note Oney***

5.3 Orders Validation

5.3.1 IPN (Instant Payment Notification) mechanism

This parameter is specifically designed to manage automatically the validation of orders issued from the merchant.

This parameter is a URL defined during the administrative registration process and stored in the merchant profile on Paybox server, but it can also be managed dynamically for every transaction by using the « PBX_REPONDRE_A » parameter.

The main role of this URL is to be called automatically (from server to server) as soon as the payment is finished (either accepted or rejected).

It allows validating automatically the corresponding order even if the customer stops the connection (browser closed) or decides not to go back to the merchant web site, because this call is going directly from Paybox platforms to the merchant system, without going to the customer´s browser.

This URL should link to a script in the Merchant environment. When calling this URL, the script will be launched, allowing the merchant to execute some operations. There are no requirements on the language of this script (ASP, PHP, PERL …). The only restriction is that this script should not make any redirection and not display an empty HTML page.

The URL specified in the IPN parameter is called for every payment attempt, whatever the number of attempts the customer has done.

This URL (IPN) has no link whatsoever with the 3 other URL parameters. It can be managed totally independently and can be called on the TCP ports 80, 443 (HTTPS), 8080, 8081, 8082, 8083, 8084 or 8085.

5.3.2 Parameters

It is possible to convert the list of parameters which will be sent back to the merchant system in the different callback URLs. This list of parameters is defined in the parameter PBX_RETOUR, by putting together the list of required information under the following Format:

```
        <name of required parameter>:<corresponding Paybox letter>;
```

Example:

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

The name of parameters (montant, maref…) can be personalized. For an overview of all the available data, please refer to the description of parameter ***PBX_RETOUR* in *§11.1.7***.

Those data are sent to all callback URLs (PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE and PBX_REPONDRE_A). For example, for the IPN URL, with the value described above, the resulting called URL would be :

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

This call is made by default using the « GET » method. If the « POST » method is preferred for transferring the parameters, this option has to be defined in the PBX_RUF1 parameter.

5.3.3 Error management

If an error occurs while calling the IPN URL, a warning email will be sent to the same email address used to send the payment tickets. For instance, if the called URL is :

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

the error message received in the email will be as follows :

> Object : PAYBOX: WARNING!!
>
> 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)**

At the end of this message between brackets **(XXX-YYY)** there will be additional information to help understanding the cause of the error:

- The first number **XXX** is the return code of the HTTP protocol
  - See the list of HTTP return codes in ***§12.2 HTTP Return codes***
  - Only the return codes beginning with ´2´ are valid.
- The second number **YYY** is the return code of the “libcurl” library in charge of message exchange with the merchant web site
  - See the list of CURL return codes in ***§12.3 CURL error codes***

5.3.4 Values checking

The IPN is called whatever the result is (accepted or rejected).

To know the result of payment, the content of the following parameters should be checked:

- Authorization number (A) : alphanumeric, variable length
  - For a test transaction (no authorization request sent to the bank or the acquirer), this parameter is always filled with « XXXXXX »
  - For a rejected transaction, this parameter is not sent back
- Error code (E) :
  - The value « 00000 » means that the transaction is accepted
  - For the other values, see ***§11.1.7 PBX_RETOUR***

To ensure that response is really coming from Paybox, it is strongly recommended to check the content of the following parameters:

- Paybox Signature (K)
  - See chapter below
- Origin IP address
  - In order to increase security, it is possible to check that the call of the IN URL comes from one of the Paybox servers (see ***§12.6 URLs to call and IP addresses***).

It will then be necessary to check the authorization number, the error code, the amount and the electronic signature: if the authorization number is existing (in the previous example, it is equal to 30258), and if the error code is equal to « 00000 », and if the amount is equal to the original amount and if the electronic signature is correct, then it means that the payment is accepted and valid.

In the case of a payment rejected by the authorization server from the acquirer, (error code is 001xx), the « xx » represent the error code sent back by this server. This code allows to know the exact reason of the rejection.
For example a transaction rejected « insufficient funds », the error code sent back would be 00151.
All possible error codes are described in ***§12.1 Response codes from the authorization center***.

5.3.4.1 Paybox Signature

By choosing the Paybox signature (letter K) in the parameters that should be sent back to the merchant system, one can make sure that :

- The integrity of the data sent back is verified,
- The call of the URL is really coming from Paybox.

It is important to notice that the data K in the parameter « PBX_RETOUR » must always be in the last position. For example:

- PBX_RETOUR=amount:M;auto:A;idtrans:S;sign:K is correct
- PBX_RETOUR=amount:M;auto:A;sign:K;idtrans:S is not correct

The Paybox public key is available for download on the website www.paybox.com in the menu« Downloads ». In order to fulfill the security rules, Paybox may change his private/public key pair. Thus, it should be possible to manage several keys in the same time in the merchant system.

- **Paybox Signature**

The Paybox signature is created by encrypting a SHA-1 hash with the private Paybox RSA key. The size of a SHA-1 hash is 160 bits and the size of the Paybox key is 1024 bits. The signature is always a binary value of fixed 128 bytes size (172 bytes in Base64 encoding).

- **Signature control**

The Paybox signature can be verified using most common languages.
For instance, with PHP, one can use the 'openssl_verify()' function and, with Java the method verify() can be used with "SHA1withRSA" option.

It is also possible to use other languages, packages, components or libraries which can handle intermediate operations (condensate or ciphering).
In any case, one has to use the Paybox public RSA key available for download.

- **Tests**

The easiest way to test a program for key verification in the merchant environment is to use a test pair of RSA keys.
It is then possible to sign messages with the private key and check the signature with the key verification program using the test public key.
Later the test public key will be replaced by the Paybox public key.

Example with OpenSSL (http://www.openssl.org/docs/apps/openssl.html) :

Generate a private RSA key *prvkey.pem* from which will be extracted aRSA public key *pubkey.pem*

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

Sign the data contained in the file *data.txt*

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

Check the signature by using the public key *pubkey.pem*

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

- **Encoding :**

Messages and signatures sent through HTTP protocol (GET or POST) need to be encoded (URL encoding and/or Base64).
Then the opposite operations have to be processed:

- Get the signature from the message,
- URL decode the signature,
- Base64 decoding of the signature,
- Verification of the signature [binary] on the data (still encoded)

With the IPN URL parameter (PBX_REPONDRE_A), the signature is only calculated on the content of the PBX_RETOUR parameter, while for the 3 other callback URLs, the signature is calculated on the entire content of the URL.

Signed data:

a) In the IPN URL, server to server call, only the data required to be sent back in the PBX_RETOUR parameter is signed,

b) For the 4 other URLs (redirection through the customer´s browser, PBX_EFFECTUE, PBX_REFUSE and PBX_ANNULE, PBX_ATTENTE), all the data following the ' ? ' (URL parameters) is signed.

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

Signature (df123dsfd3...1f1ffsre%20t321rt1t3e=) is calculated on :
Case a) pbxparam1=val1&pbxparam2=val2 ...
Case b) monparam=mavaleur& pbxparam1=val1&pbxparam2=val2 ...

NOTE: if the signature is not the last value in the PBX_RETOUR parameter, the following values will be sent back but not included in the signature.

- **Unchecked signature :**

If the checking of the signature fails, then it could be for one of the following reasons :

- Technical error : bug, cryptographic environment not correctly initialized or configured, ...
- Usage of a wrong key
- Problem with data integrity or signature tampered.

The last case is not likely to happen, but is serious. It should lead to looking for a possible intrusion into the merchant information system.

6. ADVANCED FUNCTIONALITIES

Beyond the basic payment functionality, Paybox System proposes a set of advanced functionalities providing the merchant with more flexibility to control its transactions and offering to the end customer interesting value added services.

Some of those functionalities are described below.

For an exhaustive list and a complete description of the advanced functionalities or to subscribe to some of those functionalities, please contact Sales department (see ***§9 Helpdesk - Contact***).

6.1 Integration with Paybox Direct Plus

6.1.1 How it works

By using jointly Paybox System version PLUS and Paybox Direct Plus, it is possible to have access to advanced functionalities like:

- 1 click payment,
- Delayed transaction capture,
- Authorization only
- Authorization + debit
- Debit (on a previously authorized transaction)
- Credit
- Cancellation (on a previously realized operation)
- ….

During the payment with Paybox System, card information will be saved (creation of a subscriber), and an identifier associated to this subscriber will be sent back by Paybox System (token). This will allow the merchant to use this identifier (token) later as a reference to the card information and start new payment requests using Paybox Direct Plus, without the need to provide the card information.

6.1.2 How to use

6.1.2.1 Call to Paybox System version PLUS

When calling Paybox System version PLUS, it is mandatory to use the PBX_RETOUR parameter as well as PBX_CMD and/or PBX_REFABONNE.

- One of the parameters PBX_CMD or PBX_REFABONNE must contain the identifier of the card information (or subscriber)
  - If the parameter PBX_REFABONNE is given by the merchant, this value will be used as an identifier of the subscriber (and the associated card), otherwise it will be PBX_CMD
  - It is the responsibility of the merchant to use one of those parameters and fill it with the correct value
  - This value has to be unique for a merchant contract (PBX_SITE).
- The parameter PBX_RETOUR must contain at least the data « U »
  - On the URL callback after the payment, this data « U » will be filled by Paybox with a string that the merchant must store
  - This string follows the format below, the field separator is '++' :

```
Handle_Ciphered_Card_Number++Card_Expiry_Date++CVV
```

6.1.2.2 HOW TO USE Paybox Direct Plus

In order to use with Paybox Direct Plus a subscriber previously created with Paybox System Plus :

- The parameter REFABONNE must contain the identifier of the subscriber
  - It is the value which was sent by the merchant, when calling Paybox System Plus, in the parameter PBX_REFABONNE if present or otherwise PBX_CMD
- PORTEUR should contain the handle on the ciphered card number sent back by Paybox System in the parameter U. This handle has been returned « URL encoded », it has to be « URL decoded » before to be used in Paybox Direct.
  - The card number is not complete, for security reasons.

6.1.2.3 See also

- ***[Ref 1] Manuel d'intégration Paybox Direct/Direct Plus*** for more information on this solution
- ***§11 Data dictionary***, for more information on the parameters PBX_CMD, PBX_REFABONNE, PBX_RETOUR
- ***§5 Response management***, for more information on PBX_RETOUR

6.2 Authorization without capture

6.2.1 How it works

This option allows the merchant to send an authorization request to the bank/acquirer authorization server but this transaction will never be sent to the bank for capture and the customer will never be debited if the merchant does not send to Paybox a second message requesting to capture the transaction.

This option may be used in the following scenarios:

- Debit (total or partial) after validation process,
- Debit (total or partial) at product delivery,
- Debit (total or partial) at the starting date of a service contract,
- Simple authorization to check the validity of a given card

6.2.2 How to use

By filling the parameter PBX_AUTOSEULE with 'O', only the authorization will be processed but not the capture of the transaction.
If PBX_AUTOSEULE is equal to 'N' or if the parameter is not sent in the request, the transaction will be captured automatically and uploaded to the bank during the evening process.

However, even if the transaction is processed in the «Authorization Only» mode (PBX_AUTOSEULE='O'), the transaction is duly stored and can be captured (and uploaded to the bank) later on using Batch Treatment or Paybox Direct, within a maximum delay of 75 days.

- For payment with cards, Paybox recommends to capture the transaction not more than 7 days after the associated authorization. Beyond this period, the merchant may face payment rejection for late capture.
- For payments using Paypal, the capture may occur in the next 29 days following the

authorization. However, Paypal guarantees the payments only during the next 4 days following the authorization.

- For payments using Buyster, the merchant can capture the transaction within the next 30 days after the authorization

6.3 Delayed payment

6.3.1 How it works

Paybox System can manage delayed payments, i.e. hold the transactions during several days before sending them to the bank or financial institution in order to debit the customer and credit the merchant.

This option may be very useful when the merchant wants to make sure that the service or the good has been delivered to the customer before he is debited.

On the Paybox System subscription sheet, the merchant has to define the default number of days of delayed capture that he wants to apply:

- 1 : the transaction will be uploaded to the bank the day after the payment,
- 2 : the transaction will be uploaded to the bank 2 days after the payment,
- etc…

- For payment with cards, Paybox recommends to capture the transaction not more than 7 days after the associated authorization. Beyond this period, the merchant may face payment rejection for late capture.
- For payments using Buyster, the merchant can capture the transaction within a maximum of 6 days after the authorization. Over this delay, the capture will be refused by Paybox.

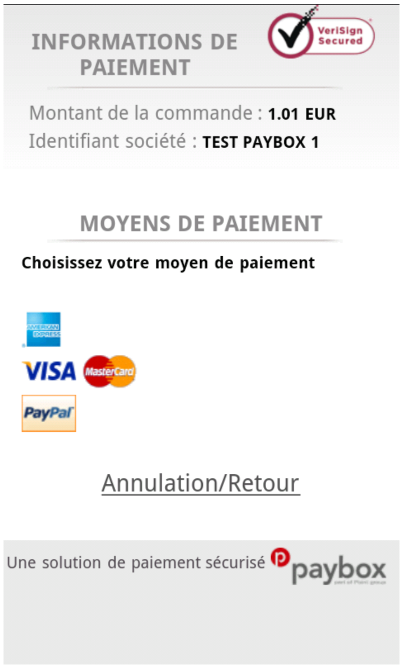
6.3.2 How to use

In the payment request, the parameter PBX_DIFF contains the number of days between the payment and the upload of the transaction to the bank. This number of days of shifting can be fixed to a default value in the subscription sheet or with the helpdesk team.

6.4 Payment on a mobile device

6.4.1 How it works

The behavior is the same as for a classical Web site on Internet. The pages displayed on the mobile or smartphone are either specific XHTML pages or pages managed by an application downloaded in the smartphone. At the payment phase, the smartphone will connect to the Paybox platform which will process the transaction as usually.
Until now, the payment methods available on mobile are : CB, VISA, MASTERCARD, AMEX, PAYPAL.



INFORMATIONS DE PAIEMENT

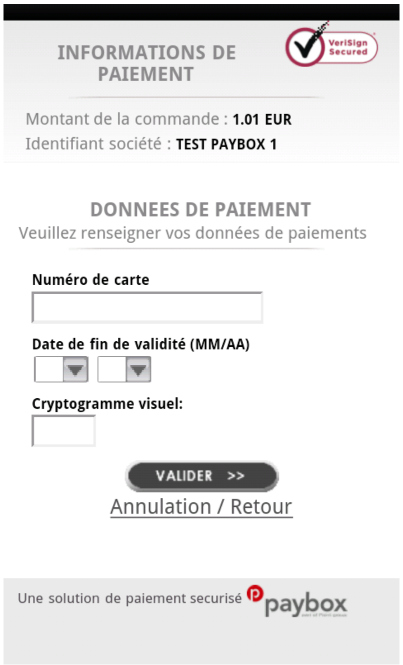
Montant de la commande : 1.01 EUR
Identifiant société : TEST PAYBOX 1

MOYENS DE PAIEMENT

Choisissez votre moyen de paiement

Annulation/Retour

Une solution de paiement sécurisé paybox



INFORMATIONS DE PAIEMENT

Montant de la commande : 1.01 EUR
Identifiant société : TEST PAYBOX 1

DONNEES DE PAIEMENT
Veuillez renseigner vos données de paiements

Numéro de carte

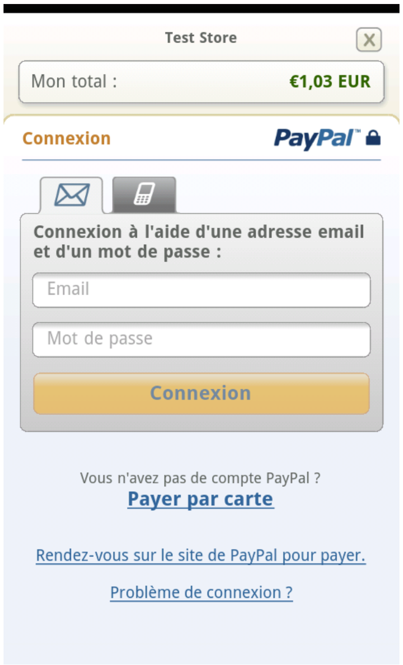
Date de fin de validité (MM/AA)

Cryptogramme visuel:

VALIDER >>

Annulation / Retour

Une solution de paiement securisé paybox



Test Store

Mon total : €1,03 EUR

Connexion PayPal

Connexion à l'aide d'une adresse email et d'un mot de passe :

Email

Mot de passe

Connexion

Vous n'avez pas de compte PayPal ?
Payer par carte

Rendez-vous sur le site de PayPal pour payer.

Problème de connexion ?

6.4.2 How to use

In the payment request, the parameter PBX_SOURCE has to be filled with the value XHTML.

NOTE: the URLs which should be called for the payment on mobile are specific. (See ***§12.6 URLs to call and IP addresses***).

7. SUBSCRIPTION MANAGEMENT

The functions described in this chapter require that the « Subscription management » option is activated for the merchant contract configuration in Paybox.

In order to subscribe to this option, please contact the Sales department (see ***§9 Helpdesk - Contact***).

7.1 How it works

The subscription functionality allows the merchant to manage recurring payments and payments in several times for his customers. Once the initial payment is done, the customer will be automatically debited upon a frequency chosen by the merchant.

- Subscription management with Paybox System is a basic function: it is able to manage simple subscription programs, based on recurring payments with the same amount at the same frequency initially defined by the merchant. Those parameters cannot be modified later on.
- However, it is possible by using jointly the delayed capture functionality to bring flexibility in the management of the date of the first payment of the subscription program.
- It should be noticed that in case a term of payment is rejected (authorization failed), Paybox will not schedule a new authorization attempt later on. The subscription program is in this case stopped and the next terms of payments will not be executed (The Paybox Direct *Plus* solution provides more flexibility on that point).
- The merchant can have a look at his ongoing subscription programs through his Back Office access.

The activation of this subscription program option has to be asked to the Sales department. Then the management of the subscription itself is done through the PBX_CMD parameter, as described below.

7.2 Creation of a subscription

The management of the subscription is done through different fields to be inserted at the end of the merchant reference order sent in the PBX_CMD parameter.
The sizes of the fields have to be respected and their names are fixed and in capital letters.

FIELD NAME	DESCRIPTION	SIZE
PBX_2MONT	Amount of the next terms of payments, in cents (0 = all amounts equal to the initial amount given in PBX_TOTAL).	10 figures
PBX_NBPAIE	Number of terms of payments (0 = never ending).	2 figures
PBX_FREQ	Frequency of terms of payments, in months.	2 figures
PBX_QUAND	Day of the month at which the term of payment will be executed (0 = same day as the initial payment).	2 figures
PBX_DELAIS	Number of days of delay before the first terms of payment is executed (beginning of subscription)	3 figures

Other fields for the payment through Paybox System do not change.

Currency is given through the parameter PBX_DEVISE and the amount of the initial payment (which can be different from the amount of the terms of payment of the subscription) is given in the parameter PBX_TOTAL.

Examples of subscription :

Example 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_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA51
2&PBX_TIME=2011-02-28T11:01:50+01:00
```

If the initial payment (15 Euros or 1500 cents) is done on the 28th of November for instance, the first term of payment will be executed on the 3rd of December (because the subscription will be delayed 5 days due to the value of PBX_DELAIS).
All the terms of payments are for an amount of 5 Euros (or 500 cents) (PBX_2MONT), executed on the 28th (PBX_QUAND) of every month (PBX_FREQ) until the subscription is cancelled by the merchant (PBX_NBPAIE=0 means that it will never end) or the card is rejected (if the card is expired for instance).

Example 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=t
est@paybox.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=20
11-02-28T11:01:50+01:00
```

If the initial payment (20 Euros, or 2000 cents) is done on the 28th of November for instance, the first term of payment will be executed on the 31st of November (because the subscription will start immediately due to the absence of PBX_DELAIS).
10 terms of payments (PBX_NBPAIE=10) for an amount of 5,50 Euros (or 550 cents) (PBX_2MONT), executed on the last day (PBX_QUAND) of every 3 months (PBX_FREQ).

When a subscription is created, a payment receipt is sent to the customer and to the merchant with information regarding the amount and the date of the next term of payment.

Content of the email sent to the customer:
Next term of payment on the xx/xx/xxxx for an amount of xx.xx Eur
(for any dispute, please contact your merchant).

Content of the email sent to the merchant:
Next term of payment on the xx/xx/xxxx for an amount of xx.xx Eur
In order to cancel this subscription, please send the PAYBOX reference xxxxxxx.

NOTE :
- When using the IPN URL, this one will be called whatever the result of the term of payment (accepted or rejected). The parameter ETAT_PBX will be added to the URL called with additional parameter PBX_RECONDUCTION_ABT.

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

7.3 Payment in several times (4 times max)

The payment in several times program has been designed for a slightly different use in comparison with the subscription program. When the subscription program is based on fixed amounts at fixed dates, the payment in several times program allows the merchant to freely configure the dates and amounts of terms of payment, within the limit of 3 payments after the initial one.

In order to use this kind of payment program, the group of parameters PBX_2MONTx and PBX_DATEx (x between 1 to 3) should be jointly sent.

<u>Example:</u>

```
PBX_SITE=1999888&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1000&PBX_DEVISE=978&PBX_CMD=TESTPaybox&P
BX_PORTEUR=test@paybox.com&PBX_RETOUR=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
```

In this example, an amount of 10 € will be immediately debited, then 20 € will be debited on the 1st of February and 30 € will be debited on the 15th of February.

As for the subscriptions, the schedule of terms of payments is managed by Paybox and once the initial payment is done, containing all the configuration information, no other call to Paybox needs to de done in order to execute the payments.

7.4 Ending of a subscription

The subscription may be ended in 3 ways:

- Normal ending

  When all the terms of payment were processed successfully, the subscription will close by itself.
- Failure ending

  When one of the terms of payment is rejected, no new attempt is scheduled. The subscription is closed and the merchant receives an email informing him about this closing and the result.
- Ending by the merchant

  The merchant can choose at any moment to stop the ongoing subscription. In order to do so, he can connect on the Back Office or send a server to server call to the paybox platform. The parameters of this call are described below.

  When the merchant closes a subscription via the Back Office, the end customer is informed by an email.

7.4.1 Ending of a subscription through a server to server call

In order to integrate the subscription management with the information system of the merchant, Paybox provides interfaces which can be called in a server to server mode, allowing the merchant to cancel an ongoing subscription.

The URL to be called is described in the chapter ***§12.6 URLs to call and IP addresses***. The call can be sent with a GET or a POST method and should contain a string which is a list of fields.

The subscription to be cancelled can be identified in 2 ways:

- By subscription number

  This number is sent back by Paybox System in the field ABONNEMENT

  Example:

  `VERSION=001&TYPE=001&SITE=1999888&MACH=099&IDENTIFIANT=2&ABONNEMENT=1`

- By reference order

  It is the reference sent by the merchant when calling Paybox System

  Example:

  `VERSION=001&TYPE=001&SITE=1999888&MACH=099&IDENTIFIANT=2&REFERENCE=refcmd`

In response, the server will also send a string of fields. The ACQ fields allow the merchant to know the result of the cancellation of the subscription.
Furthermore, the order reference sent by the merchant in the original call is sent back in the answer in the parameter ABONNEMENT or REFERENCE.

Examples:

Answer in case of success: `ACQ=OK&IDENTIFIANT=2&ABONNEMENT=1`
Answer in case of failure: `ACQ=NO&ERREUR=9&IDENTIFIANT=2&REFERENCE=refcmd1`

NOTE: no email is sent to the customer when the cancellation of the subscription is done in the server to server mode.

8. MERCHANT BACK-OFFICE

Once the merchant has been registered within Paybox, he automatically gets an access to the Merchant Back Office secure on-line dashboard allowing the merchant to have a look at his transactions, sales figures … and providing him with the possibility to execute various actions (exports, cancel/refund transactions, management of delayed capture …).

8.1 Access and functionalities

Access conditions to the Merchant Back Office and an explanation of the full set of available functionalities are described in the document ***[Ref 2] Guide Utilisateur du Back Office,*** available here: http://www1.paybox.com/espace-integrateur-documentation/manuels/?lang=en

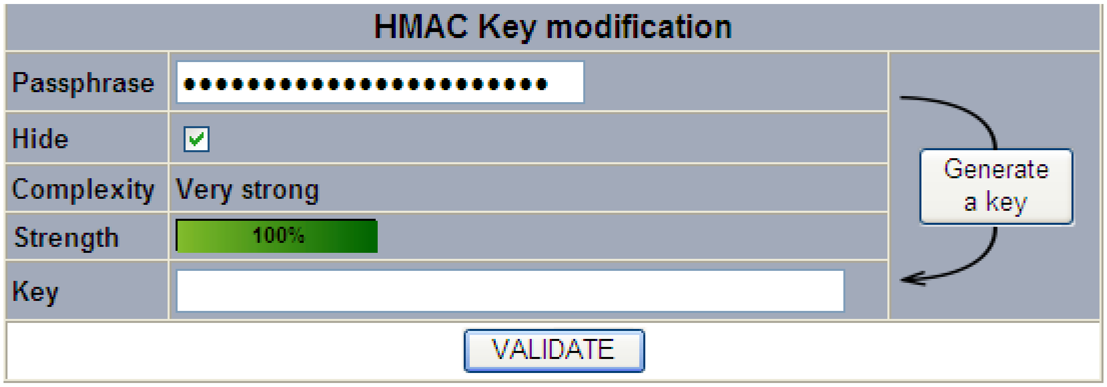
8.2 Management of the HMAC authentication key

This key is absolutely mandatory. It allows the merchant to be fully identified by Paybox when its application is interacting with Paybox. All the messages exchanged between the merchant and Paybox will be authenticated. The merchant has to generate his own secret key and use it to calculate a HMAC hash for every of the messages sent.

8.2.1 Key generation

The interface from which the authentication key can be generated is in the menu « Information » of the Merchant Back Office, at the bottom of the page.

This interface looks like this:



HMAC Key modification

Passphrase	●●●●●●●●●●●●●●●●●●●●●●●●
Hide	☑
Complexity	Very strong
Strength	100%
Key	

Figure 4 : Generating a secret key

The field « Passphrase » can be filled with a sentence, a password or any other text.

The content of the field « Passphrase » is hidden by default, characters appear like a password. It is possible to choose to see the content of this filed by un-checking the field "Hide".

The fields « Complexity » and « Strength » are automatically updated when the passphrase is entered. Those fields indicate the security level of the passphrase entered. The security rules require to enter a passphrase of minimum 15 characters long and with a strength of minimum 90%. The button « VALIDATE » will stay inactive until this security level is reached.

The strength of the passphrase is calculated upon different parameters as the number of uppercase letters, lowercase letters, specific characters, etc … It is then necessary to enter a passphrase containing various type of characters and to alternate in order to avoid repetitive sequence of characters which reduce the strength.

The button « Generate a key » allows generating the authentication key from the entered passphrase. The method used to generate the key is a standard. If the same passphrase is entered 2 times, the calculation will give the same key as a result.

- ❗ NOTE: it is possible that the key generation takes a few seconds, depending on the Internet browser used and the power of the computer. During the calculation, it is possible that the browser asks if it should “stop the execution of this script”. It is necessary to answer “No” and wait until the end of the calculation.

Once the key calculation is finished, the key will be displayed in the field « Key ». It is then possible to copy/paste this key in order to store it into the information system of the merchant, for example into a database, preferably in a secure way.

It is also possible to directly fill the field « Key » with his own authentication key (in hexadecimal format) calculated by another method. The minimum size of key to be entered corresponds to a result key generated from a SHA-1 calculation, so 40 hexadecimal characters. However, if this method of entering an “external” key is used, an alert will be displayed explaining that Paybox cannot guarantee the strength of this key.

The button « VALIDATE » is inactive by default. The 2 events which can switch it to active state are :

- Enter a passphrase of minimum 15 characters and with a strength of minimum 90%
- Enter an hexadecimal authentication key of minimum 40 characters

After entering the elements which fulfill the minimum criteria, if the button “VALIDATE” is clicked directly (without clicking on « generate a key »), the calculation of the key will start directly.

After validation of the key generation, a message will be displayed explaining that an email has been to the merchant email address for confirmation. The generated key will not be active until the indications given in this email are not executed.
For security reasons, the key will not be any more displayed in the Back Office and neither given by the support team. If the key is lost, it will be necessary to generate a new one. For those reasons, it is important to save the key generated before leaving the Back Office.

- ❗ NOTE: the key is associated to the platform on which it has been generated. It means that after the merchant generates a key on the pre-production platform for his integration tests, a new key has to be generated and used on the production platform before going live.

8.2.2 Validation

Once the key is generated, an email is automatically sent to the merchant. This email will contain a link to the program « CBDValid.cgi », for instance :

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

The parameter « id » is not the key but a token generated randomly and associated to the key which should be validated. As said previously, the key will not be sent in the email.

After clicking on the link, a message is displayed confirming « Your key is now active », which means that the key is now valid. This also means that the merchant should make sure that this key is active in his system.

The key should be activated within 31 days after its creation. Once this delay is expired, the key cannot be activated and a new key should be generated.

8.2.3 Expiry

There is no expiration date for the key. Once activated, the key will always be valid.

However, Paybox recommends changing this key regularly, once a year for example.

8.2.4 Transmission

The secret key used for authentication should never be transmitted by e-mail. Paybox will never ask the merchant for this key. Merchants should be careful not to disclose the key to anybody asking for it. This is most likely a case if phishing or social engineering.

When the key is lost, Paybox is not able to provide the value of the key. You can simply regenerate a new key in the merchant Back Office environment.

9. HELPDESK - CONTACT

9.1 Access

INFORMATION

For any information requests from merchants or integrators, the Sales team is available from Monday to Friday, from 9am to 6pm:

Sales team :

E-mail: contact@paybox.com

Phone: + 33 (0)1 61 37 05 70

SUPPORT

For any information or help request regarding the installation, configuration or use of our solutions, our Helpdesk team is available for merchants and integrators from Monday to Friday, from 9am to 12.30am and from 2pm to 6.30pm (5.30 on Friday) :

Technical & Functional support:

E-mail: support@paybox.com

Phone: + 33 (0)4 68 85 79 90

For any contact with Sales team or Helpdesk team, following information is MANDATORY, in order to correctly identify the issuer of the request:

- SITE number (7 digits)
- RANK number (2 digits)
- Paybox identifier (1 to 9 digits)

9.2 Functions

The functions of the support team are :

- Integration and maintenance support for merchants
- Process survey
- Jointed analysis with different other teams (R&D, Admins, Network, …) to find out causes of problems

9.3 Merchant subscription procedure

In order for the merchant to subscribe to Paybox solutions and services, the merchant must contact the Sales department (see contact details above), or get in contact with Paybox by filling the contact form available in the « ***Contact*** » menu in the Paybox web site ***www.paybox.com***, or send an email to **contact@paybox.com.**

The merchant will then receive a subscription form that he should fill with the required information and send back to Paybox.

Prior to do so, the merchant should contact his bank or private acquirer and ask for opening and delivery of a merchant contract number for payments in E-Commerce (Card Non Present) mode. The conditions associated to this kind of contract may vary for every bank/acquirer.

The bank will then provide the merchant with a merchant contract number corresponding to the parameter SITE (usually on 7 digits) and a rank number corresponding to the parameter RANG (2 or 3 digits) : those 2 information will allow Paybox to identify the merchant.

Information to be filled in the subscription form is :

- Merchant contact details,
- Contact details of the company hosting the web site (if the merchant does not host his platform himself),
- merchant contract information (provided by the bank),

If the merchant wants to accept payments in other currencies than Euros, it should be specified when opening the merchant contract number with the bank and when filling the subscription form for Paybox.

For other payment methods, the merchant may contact the Paybox Sales department who will explain the specificities corresponding to every one of those methods.

10. TEST ENVIRONMENT

Before starting to make payments live in production, Paybox strongly recommends to the merchant to check the correct integration of the Paybox solutions by doing some tests in the pre-production environment.

Paybox provides a PCI DSS pre-production environment and test accounts and parameters fully dedicated to the tests and integration.

All information related to this pre-production environment is described in the following document [Ref1] « ParametresTestPaybox_V6.1_EN.pdf » available for download here:
http://www1.paybox.com/espace-integrateur-documentation/manuels/?lang=en

11. DATA DICTIONARY

The complete list of Paybox System parameters is defined below. For each of them, a detailed description (format, content, examples) is given in the following pages.

PARAMETER	DESCRIPTION	P
PBX_1EURO_CODEEXTERNE	Specific data for 1euro.com	C
PBX_1EURO_DATA	Specific data for 1euro.com	C
PBX_2MONT*n*	Several times payment : amount of terms of payment	O
PBX_3DS	Temporary 3-D Secure deactivation	O
PBX_ANNULE	Callback URL in case of transaction aborted/cancelled	O
PBX_ARCHIVAGE	Archiving reference	O
PBX_ATTENTE	Callback URL in cas of transaction waiting confirmation	
PBX_AUTOSEULE	Authorization only (no capture)	O
PBX_CK_ONLY	Force the payment with only gift cards	O
PBX_CMD	Order reference	**M**
PBX_CODEFAMILLE	Specific data for Cofinoga	C
PBX_CURRENCYDISPLAY	Configuration of currencies display	O
PBX_DATE*n*	Several times payment : date of terms of payment	O
PBX_DEVISE	Currency	**M**
PBX_DIFF	Number of days of shifting in case of delayed payment	O
PBX_DISPLAY	Payment page Timeout	O
PBX_EFFECTUE	Callback URL in case of transaction accepted	O
PBX_EMPREINTE	Hash given after a payment	O
PBX_ENTITE	Numeric reference for subdivision (geographical, organizational …)	O
PBX_ERRORCODETEST	Error code to send back (for tests)	O
PBX_GROUPE	Merchant group for Paybox Version ++	C
PBX_HASH	Algorithm used to calculate the HMAC hash	**M**
PBX_HMAC	Message hash	**M**
PBX_IDABT	Subscription number	O
PBX_IDENTIFIANT	Paybox identifier	**M**
PBX_LANGUE	Payment page language	O
PBX_MAXICHEQUE_DATA	Specific data for Maxichèque	C
PBX_NBCARTESKDO	Maximum number of gift cards for 1 payment	O

PBX_NETRESERVE_DATA	Specific data for Net Reserve	C
PBX_ONEY_DATA	Specific data for Oney	C
PBX_PAYPAL_DATA	Specific data for Paypal	C
PBX_PORTEUR	E-mail address of the customer	**M**
PBX_RANG	Rank number provided by the bank	**M**
PBX_REFABONNE	Subscriber reference (version Plus)	C
PBX_REFUSE	Callback URL in case of payment rejected	O
PBX_REPONDRE_A	IPN URL	O
PBX_RETOUR	Data configuration in the answer	**M**
PBX_RUF1	Calling method for the IPN URL	O
PBX_SITE	Merchant contract number provided by the bank	**M**
PBX_SOURCE	Format of the payment page (for payment on mobile)	O
PBX_TIME	Timestamp of the message (and of the hash)	**M**
PBX_TOTAL	Amount	**M**
PBX_TYPECARTE	Card type forcing	O
PBX_TYPEPAIEMENT	Payment type forcing	O

Array 1 : List of Paybox System parameters

Caption : M = Mandatory ; O = Optional ; C = Conditional

11.1 Mandatory parameters for Paybox System

11.1.1 PBX_SITE

Format: 7 digits. **Mandatory.**

Merchant contract number provided by the bank.

Example: 1999888

11.1.2 PBX_RANG

Format: 2 digits. **Mandatory.**

Rank number provided by the bank.

Example: 01

11.1.3 PBX_TOTAL

Format System : 3 to 10 digits. **Mandatory.**
Format Direct: 10 digits. **Mandatory.**

Total amount of the transaction, in cents of the currency of the transaction (no comma, no point).

Example: for 19 € 90 :

- 1990

11.1.4 PBX_DEVISE

Format: 3 digits. **Mandatory.**

Currency of the transaction according to ISO 4217 norm (numeric code)

Examples :

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

NOTE : Before to realize payments in different currencies, the merchant should check with his bank that the merchant number allows payments in those different currencies.
Some payment means accept only Euro currency. In that case, when trying to pay in other currency, they are not proposed on the page displayed for the selection of payment method.

11.1.5 PBX_CMD

Format: 1 to 250 characters. **Mandatory.**

It is the reference of the order, given by the merchant. This parameter allows the merchant to make a link between the products bought on his Web shop and the associated payments. This parameter has to be unique for each call.

In the case of using Paybox System version PLUS, this value can also be used as a reference on the subscriber and can be reused in Paybox Direct Plus.

Example: CMD9542124-01A5G

11.1.6 PBX_PORTEUR

Format: 6 to 120 characters. **Mandatory.** The characters « @ » and « . » must be present.

Email address of the customer (cardholder).

Example: test@paybox.com

11.1.7 PBX_RETOUR

Format: <field name>:<letter>; **Mandatory.**

Data fields returned by Paybox.

See also:

§5 Response management

Below, a complete list of the available fields :

CODE	DESCRIPTION
M	A**M**ount of the transaction (given in PBX_TOTAL).
R	**R**eference of the order (given in PBX_CMD) : space URL encoded
T	Paybox Call Number
A	**A**uthorization number (reference given by the authorization center) : URL encoded
B	Su**B**scriber number (given by Paybox)
C	**C**ard type (cf. PBX_TYPECARTE)
D	**D**ate of expiry of the card. Format: YYMM
E	Response code of the transaction (cf.**§12.1 Response codes from the authorization center**)
F	Status of authentication of the cardholder in 3-D Secure program : • Y:Cardholder authenticated • A: Cardholder authentication forced by the issuer bank • U:Cardholder authentication could not be realized • N: Cardholder not authenticated
G	**Gu**arantee of the payment in 3-D Secure program. Format: O (Yes) or N (No)
H	Card **H**ash
I	Country code of **I**P address of the cardholder. Format: ISO 3166 (alphabetical)
J	2 last digits of the PAN (card number)
K	Signature of the fields in the URL. Format: url-encoded
N	6 first digits (« bi**N**6 ») of the PAN (card number)
O	Cardholder Enr**O**lment to the 3-D Secure program : • Y:Cardholder enrolled • N: Cardholder not enrolled • U:Unknown information
o	Payment option chosen by the customer : • 005 : Cash • 001 : Credit
P	**P**ayment type (cf. PBX_TYPEPAIEMENT)
Q	Transaction timestamp. Format: HH:MM:SS (24h)

S	Paybox Tran**S**action number
U	Subscription management with Paybox Direct Plus. For payments with card : `Ciphered_Card_Number_Handle++Card_Expiry_Date++---` This field is URL encoded. This value has to be be saved. For payments with Paypal : This field contains the authorization identifier given by Paypal. It is not necessary for later payments.
W	Transaction processing date on the Paybox platform. Format: DDMMYYYY
Y	Country code of the card issuer bank. Format: ISO 3166 (alphabetical)
Z	Index used for mix payments (gist card associated with a complement as CB/Visa/MasterCard/Amex)

Array 2 : Fields PBX_RETOUR

CODE	DESCRIPTION
00000	Successful operation.
00001	Connection to the authorization center failed or an internal error occurred. In this case, it is advised to try on the backup site: tpeweb1.paybox.com.
001xx	Payment rejected by the authorization center [see **§12.1 Response codes from the authorization center**].
00003	Paybox error. In this case, it is advised to try on the backup site: tpeweb1.paybox.com.
00004	Card number invalid or visual cryptogram invalid
00006	Access refused or site/rank/identifier incorrect.
00008	Incorrect expiry date.
00009	Error when during subscriber creation
00010	Unknown currency
00011	Amount incorrect.
00015	Payment already done.
00016	Subscriber already exists (registration of a new subscriber). Value 'U' of PBX_RETOUR.
00021	Not authorized bin card.
00029	Not the same card used for the first payment. Error code associated with the variable "PBX_EMPREINTE".
00030	Time-out > 15 mn before validation by the buyer when the buyer is on the page of payments of PAYBOX.
00031	Reserved
00032	Reserved

00033	Unauthorized country code of the IP address of the cardholder's browser.
00040	Operation without 3DSecure authentication, blocked by the fraud filter.
99999	Payment waiting confirmation from the issuer

Array 3 : PBX_RETOUR response codes

11.1.8 PBX_IDENTIFIANT

Format: 1 to 9 digits. **Mandatory.**

Paybox identifier given by Paybox to the merchant during registration process.

Example: 200814357

11.1.9 PBX_HASH

Format: Text. **Mandatory.**
Default value : SHA512

Defines the hash algorithm used when calculating the HMAC hash.

This algorithm has to be chosen within the following list :

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

Hash with MD2/4/5 algorithm is too weak and will not be accepted.

PBX_HASH should be filled with one value of this list, in capital letters and the algorithm defined here should be the one used for the calculation of the hash.

11.1.10 PBX_HMAC

Format: Text (hexadecimal format). **Mandatory.**

Allows checking the merchant authentication and the message integrity. It is calculated from the list of other parameters sent in Paybox system request.

See also:

- **§4.3 Message authentication with HMAC hash**

11.1.11 PBX_TIME

Format: Date ISO8601 format. **Mandatory.**

Timestamp of the HMAC calculation. Has to be URL encoded.

11.2 Optional parameters for Paybox System

The following parameters are classified in alphabetical order.

11.2.1 PBX_ARCHIVAGE

Format: up to 12 alphanumeric characters

Transaction reference sent to the bank during transaction upload. It should be unique and may allow the bank and the merchant to match transactions together.

11.2.2 PBX_AUTOSEULE

Format: O (Yes) or N (No)
Default value: N

If filled with « O », the transaction will be processed for authorization only. It will not be uploaded to the bank at evening.

However, the authorization will be stored and it will be possible, using Paybox Batch Processing or Paybox Direct, to capture the transaction later on, in order to upload it to the bank.

11.2.3 PBX_ANNULE

Format: up to 150 characters
Default value: value stored in the merchant profile when registering in Paybox

Callback URL towards the page to which the cardholder will be redirected after the payment has been aborted/cancelled.

Fields defined in PBX_RETOUR will be sent to this page.

Example: http://www.commerce.fr/annulation.html
See also:

- **§5 Response management**

11.2.4 PBX_ATTENTE

Format: up to 150 characters
Default value : value stored in the merchant profile when registering in Paybox

Callback URL towards the page to which the cardholder will be redirected after the payment has been completed but is awaiting confirmation from the issuer.

Fields defined in PBX_RETOUR will be sent to this page.

Example: http://www.commerce.fr/attente.html
See also:

- **§5 Response management**

11.2.5 PBX_CURRENCYDISPLAY

Format: up to 23 characters (6 x 3 codes separated with comma)
Default values : all currencies are displayed

List of currencies to be displayed on the payment page.

Available currency codes are as follow :

- EUR : Euro
- CHF : Swiss Franc
- USD : US Dollar
- JPY : Yen
- CNY : Yuan
- GBP : Sterling Pound
- CAD : Canadian Dollar
- NO_CURR : specific value to display no currency

Example: `EUR,USD,GBP`

11.2.6 PBX_DATEVALMAX

Format: Date in YYMM format

Expiry date not to be exceeded.

If the date of expiration of the card is lower than the limit fixed by this variable, the payment will be refused. This is useful in the case of payments n time and to avoid that a reconduction fails because of expiry date is < at the last reconduction

Example:
Scheduled payments 04/05/2013, 08/06/2013 and 30/07/2013
PBX_DATEVALMAX=1307
If the card expires before july 2013, the initial payment will be refused with error code 00008.

11.2.7 PBX_DATE1, PBX_DATE2, PBX_DATE3

Format: Date in DD/MM/YYYY format

Date of the second term of payment for a payment in several times (respectively 3rd and 4th terms of payment for PBX_DATE2 et PBX_DATE3).

Those parameters have to be used jointly with PBX_2MONT1, PBX_2MONT2, PBX_2MONT3.

Example: 30/06/2012
See also:

- **§7.3 Payment in several times (4 times max)**
- **§11.2.23 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3**

11.2.8 PBX_DIFF

Format: 2 digits

Number of days for the delay between payment and capture (upload to bank).

It is possible to cancel this delay from the merchant back office. For example, a transaction carried out on November 2nd, and deferred until November 4th, can be released and sent manually on November 3rd.

A default value for this parameter may have been defined in the merchant profile when registering at Paybox. If this parameter is sent in the call to Paybox System, the value in the call is priority to the one in the merchant profile.

Example: 04 for a 4 days delay
See also:

- **§6.3 Delayed payment**

11.2.9 PBX_DISPLAY

Format: 3 to 10 digits
Default value : 900

TimeOut for the payment page (in seconds). Once this timeout has exceeded, the transaction is considered aborted.

11.2.10 PBX_EFFECTUE

Format: up to 150 characters
Default value : value stored in the merchant profile when registering in Paybox

Callback URL towards the page to which the cardholder will be redirected after the payment has been aborted/cancelled.

Fields defined in PBX_RETOUR will be sent to this page.

Example: http://www.commerce.fr/confirmation.html
See also:

- ***§5 Response management***

11.2.11 PBX_EMPREINTE

Format: 64 characters

Digest provided by PAYBOX at the moment of the first payment via the variable ‘H’ of « PBX_RETOUR ».

11.2.12 PBX_ENTITE

Format: 1 to 9 digits

Numeric reference of a geographic subdivision, functional, sales, …

11.2.13 PBX_ ERRORCODETEST

Format: 5 digits

Error code to return in the pre-production/tests environment.

Parameter ignored in the production environment.

See also:

§11.1.7 Array 3 : PBX_RETOUR response codes

11.2.14 PBX_GROUPE

Format: up to 10 digits

Mandatory variable for use with the Paybox Version++ solution

Defines a group of merchants which can re-use the same subscriber reference to charge the same client.

11.2.15 PBX_IDABT

Format: 9 digits

Subscription number sent with the variable ‘B’ of PBX_RETOUR.

The value filled into this parameter will update the card number of the subscriber if the payment is authorized and if the subscription is valid.

The subscription has been created by the product PAYBOX SYSTEM.

See also:

- ***§7 Subscription management***

11.2.16 PBX_LANGUE

Format: 3 characters
Default value : FRA

Language used by Paybox to display the text on the payment page

Possible values:

- FRA : French
- GBR : English
- ESP : Spanish
- ITA : Italian
- DEU : German
- NLD : Dutch
- SWE : Swedish
- PRT : Portuguese

11.2.17 PBX_REFABONNE

Format: up to 250 characters

Subscriber reference given by the merchant when using the Paybox Direct Plus or Paybox System version PLUS products.

Filling this parameter allows to replace the card number associated to a previously registered subscriber or to create it if he does not exist yet.

See also:

- ***§6.1 Integration with Paybox Direct Plus***

11.2.18 PBX_REFUSE

Format: up to 150 characters
Default value : value stored in the merchant profile when registering in Paybox

Callback URL towards the page to which the cardholder will be redirected after the payment has been refused.

Fields defined in PBX_RETOUR will be sent to this page.

Example: http://www.commerce.fr/refus.html
See also:

- ***§5 Response management***

11.2.19 PBX_REPONDRE_A

Format: up to 150 characters
Default value : value stored in the merchant profile when registering in Paybox

Server to server callback URL, also called IPN (Instant Payment Notification), caklled immediately after each payment attempt, whatever the result is. It allows the merchant to manage safely the validation of the orders.

Fields defined in PBX_RETOUR will be sent to this page.

Example: http://www.commerce.fr/validation_paiement.cgi
See also:

- ***§5 Response management***

11.2.20 PBX_RUF1

Format: « GET » or « POST »
Default value : GET

Method (in HTTP protocol meaning) used to call the IPN URL.

See also:

- ***§5 Response management***
- **§11.2.18 PBX_REPONDRE_A**

11.2.21 PBX_SOURCE

Format: 3 to 5 characters.
Default value : HTML

Defines the format of the page where the payment method is selected. This value depends on the type of browser used. Possible values are :

- HTML : for PCs
- WAP : WML format, for WAP compliant smartphones
- IMODE : iHTML format
- XHTML : light page, adapted for mobile phones (smartphones/ tablets)

NOTE: Paybox does not detect automatically the browser

11.2.22 PBX_TYPEPAIEMENT

Format: 5 to 10 characters.
Default value : <empty>

Allows to preselect a payment method.

- On the payment method selection page : allows to display only the given payment methods
  - If the merchant has got the Paypal option activated but he wants to offer only payment by card for a kind of goods, he should then fill this parameter with « CARTE ».
  - Then, only the payment methods using cards will be displayed on the selection page
- On the payment page: used with PBX_TYPECARTE, allows to not display the selection page and to display directly the payment page adapted to the 2 parameters.

See also:

§11.2.23 PBX_TYPECARTE

11.2.23 PBX_TYPECARTE

Format: min. 2 characters.
Default value : <empty>

Defines the card type to be used on the payment page in case the selection page proposed by Paybox is not used.
Should always be used jointly with PBX_TYPEPAIEMENT.

PBX_TYPEPAIEMENT	PBX_TYPECARTE
CARTE	CB, VISA, EUROCARD_MASTERCARD, E_CARD
	MAESTRO
	AMEX
	DINERS
	JCB
	COFINOGA
	SOFINCO
	AURORE
	CDGP
	24H00
	RIVEGAUCHE
	BCMC
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

Array 4 : Possible values for PBX_TYPEPAIMENT and PBX_TYPECARTE

11.2.24 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3

Format: 3 to 10 digits

Amount in cents (without comma or point) of the next terms of payments for a several times payments. Subscriber management option should be activated.
Those parameters have to be used jointly with PBX_DATE1, PBX_DATE2, PBX_DATE3.

See also:

- ***§7.3 Payment in several times (4 times max)***
- ***§11.2.7***

PBX_DATE1, PBX_DATE2, PBX_DATE3

11.2.25 PBX_3DS

Format: 'N' : No 3-D Secure authentication of the cardholder

Allows to not ask for 3D Secure authentication, only for this transaction, even if the merchant and the card holder are enrolled in 3D Secure program.
Not fill this parameter if the 3D Secure authentication is requested by the merchant.

See also:

- A definition of 3DSecure in ***§12.7.1 3-D Secure***

11.3 Specific parameters for some type of cards

11.3.1 PBX_1EURO_CODEEXTERNE

Format: 3 digits. Only for payment with « 1Euro.com ».

External promotional code.

11.3.2 PBX_1EURO_DATA

Format: up to 100 characters. Only for payment with « 1Euro.com ».

Identification data for customer localization.
Fields are separated with # and have to respect the following order :

1. Civility,
2. Last name,
3. First name,
4. Address1,
5. Address2,
6. Address3,
7. Postal Code,
8. City,
9. Country Code (FR for France),
10. Home phone number,
11. Mobile phone number,
12. Flag indicating if the merchant knows the cardholder (0 : unknown, 1 : known),
13. Flag indicating if the merchant has already had some problems of payment with this cardholder,
14. COFIDIS action code (fixed value provided by COFIDIS)

Example:

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

11.3.3 PBX_CKONLY

Format: O or N. Only for gift cards.

Use the value “O” to force the payment only with gift cards. Else, the client can use his credit card or another payement method to complete the payment.

11.3.4 PBX_CODEFAMILLE

Format: 3 digits. Only for payments with SOFINCO, COFINOGA or CDGP.

Value filled by the merchant to indicate which commercial option he wants to propose to the customer when paying with SOFINCO card (or partner card SOFINCO), COFINOGA or CDGP.

11.3.5 PBX_MAXICHEQUE_DATA

Format: up to x digits. Only for payment with MAXICHEQUE.

Describes the family of the product bought. See Maxichèque documentation for more details.

11.3.6 PBX_NBCARTESKDO

Format: up to 2 digits. Only for gift cards.

Controls the number of gift cards that a client can use for an unique payment.

Values allowed are between 1 and 25.

11.3.7 PBX_NETRESERVE_DATA

Format: up to 250 characters. Only for payments with Net Reserve.

Identification data for customer localization.
Fields are separated with # and have to respect the following order :

1. First name (25 characters),
2. Last name (25 characters),
3. Address1 (25 characters),
4. Address2 (25 characters),
5. Postal code (10 characters),
6. City (25 characters),
7. Country code (2 characters : FR for France),
8. Email (50 characters),
9. Telephone (25 characters)

Example:

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

11.3.8 PBX_OPECOM

Format: 5 digits. Only for FINAREF payments with card SURCOUF
Format: 10 characters. Only for the « 34ONEY » application

Commercial option.

11.3.9 PBX_ONEY_DATA

Format: Characters. Only for the « 34ONEY » application.

For more information about the integration of this payment method, please refer to the document ***[Ref 10] Note Oney***

11.3.10 PBX_PAYPAL_DATA

Format: up to 490 characters.

Only for payments with Paypal : identification data for customer localization.

Fields are separated with # and have to respect the following order :

- ✓ Customer name (32 characters),
- ✓ 1st line of address (100 characters),
- ✓ 2nd line of address (100 characters) ,
- ✓ City (40 characters),
- ✓ State / Region (40 characters),
- ✓ Postal code(20 characters),
- ✓ Country code (FR for France) (2 characters),
- ✓ Telephone number (20 characters)
- ✓ Payment description (127 characters)

The last parameter "Payment description" is mandatory in case of payment using subscriber option (Paybox System version PLUS), but it is recommended to provide it even in other cases.

Example:

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

11.4 Paybox System – Cancelling Subscription : Request

11.4.1 VERSION

Format: 3 digits. **Mandatory.**
Default value : 001

Protocol version : 001

11.4.2 TYPE

Format: 3 digits. **Mandatory.**
Default value : 001

Request type : 001 = Cancelling

11.4.3 SITE

Format: 7 digits. **Mandatory.**

Site number.
Same value as for a standard call to Paybox System.
Provided by Paybox to the merchant during registration process.

11.4.4 MACH

Format: 3 digits. **Mandatory.**

Rank number.
Same value as for a standard call to Paybox System.
Provided by Paybox to the merchant during registration process.

11.4.5 IDENTIFIANT

Format: 1 à 9 digits. **Mandatory.**

Paybox identifier.
Same value as for a standard call to Paybox System.
Provided by Paybox to the merchant during registration process.

11.4.6 HMAC

Format: Text. **Mandatory.**

Allows to check merchant authentication and message integrity. Calculated with the same method as for a standard call to Paybox System.

See also:
§4.3 Message authentication with HMAC hash

11.4.7 TIME

Format: Date in ISO8601 format. **Mandatory.**
Timestamp of HMAC calculation.

11.4.8 ABONNEMENT

Format: 1 to 9 digits. **Mandatory if no reference provided (REFERENCE).**

Reference number of subscription to be cancelled.

11.4.9 REFERENCE

Format: 1 to 250 characters. **Mandatory if no subscriber number provided (ABONNEMENT).**

Reference of subscription to be cancelled.

11.5 Paybox System – Cancelling Subscription: Answer

The answer contains parameters indicating if the cancellation has succeeded or not, the failure reason in case of failure and some data from the original request.

11.5.1 ACQ

Format: 2 characters. **Mandatory.**

OK : Successfull
NO : Failure

11.5.2 ERREUR

Format: 1 digit. **Mandatory in case of failure.**

Error number in case of failure :

- 1 : Technical problem (Configuration),
- 2 : No coherent data,
- 3 : Technical problem (Database access),
- 4 : Unknown site,
- 9 : Cancellation failure. Subscription has not been cancelled.

11.5.3 IDENTIFIANT

Format: 1 to 9 digits. **Mandatory.**

Value sent in the initial request.

11.5.4 ABONNEMENT

Format: 1 to 9 digits. **Mandatory if no reference provided (REFERENCE).**

Value sent in the initial request.

11.5.5 REFERENCE

Format: 1 to 250 characters. **Mandatory if no subscriber number provided (ABONNEMENT).**

Value sent in the initial request.

12. ANNEXES

12.1 Response codes from the authorization center

This information is sent back in the answer to the merchant at the end of the transaction if it has been required by sending the parameter E in the call.

See ***§11.1.7 PBX_RETOUR*** and ***§5 Response management***

12.1.1 Card schemes Carte Bancaire, American Express and Diners

CODE	MEANING
00	Transaction approved or successfully processed.
01	Contact the card issuer.
02	Contact the card issuer.
03	Invalid retailer.
04	Keep the card.
05	Do not honor.
07	Keep the card, special conditions.
08	Approve after holder identification.
12	Invalid transaction.
13	Invalid amount.
14	Invalid holder number.
15	Card issuer unknown.
17	Client cancellation.
19	Repeat the transaction later.
20	Error in reply (error in the server’s domain).
24	File update not withstood.
25	Impossible to situate the record in the file.
26	Record duplicated, former record replaced.
27	Error in ‘edit’ in file update field.
28	Access to file denied.
29	File update impossible.
30	Error in format.
33	Expired card
38	Too many attempts at secret code.

41	Lost card.
43	Stolen card.
51	Insufficient funds or over credit limit.
54	Expiry date of the card passed.
55	Error in secret code.
56	Card absent from file.
57	Transaction not permitted for this holder.
58	Transaction forbidden at this terminal.
59	Suspicion of fraud.
60	Card accepter must contact purchaser.
61	Amount of withdrawal past the limit.
63	Security regulations not respected.
68	Reply not forthcoming or received too late.
75	Too many attempts at secret code.
76	Holder already on stop, former record kept.
89	Authentication failure
90	Temporary halt of the system.
91	Card issuer not accessible.
94	Request duplicated.
96	System malfunctioning.
97	Time of global surveillance has expired.

Array 5 : Response codes from authorization center

12.1.2 Card schemes Cetelem/Aurore and Rive Gauche

CODE	MEANING
00	Transaction approved or successfully processed.
01	Retailer’s number incorrect or unknown.
02	Incorrect card number
03	Error in date of birth or secret code.
04	Card non financially viable
05	Problem at the CETELEM server center
06	Card unknown.
07	Request for reserve refused.
08	Card out of date.

09	Card / retailer non-compatible.
10	Unknown.
11	Cancelled.
12	Incorrect currency code.
13	Transaction reference not recorded.
14	Incorrect transaction amount.
15	Incorrect terms of payment
16	Incorrect transaction direction
17	Incorrect payment mode

Array 6 : Response codes from the Cetelem authorization center

12.1.3 Card scheme Finaref

CODE	MEANING
000	OK
101	Card expired
103	Unknown merchant. Incorrect merchant identifier
110	Invalid amount
111	Unknown cardholder/account
115	Service not available. Null limit. Unknown function/treatment code
116	Insufficient funds
117	1st or 2nd invalid secret code
119	Cardholder/account blocked. Cardholder/account invalid. Card blocked
120	Invalid merchant. Incorrect currency code. Account not authorized. Unknown/invalid commercial operation.
121	Insufficient limit
125	Card inactive
126	Secret code absent. Invalid format of the date of beginning of control or of the security information.
128	Error of control of the incorrect secret code history.
129	Incorrect CVV2
183	Account / Cardholder invalid.
184	Inconsistency of validity date with the cardholders files in manual entry
188	Invalid entry mode. Inconsistent equipment identification.
196	Problem while accessing files.
206	3rd invalid secret code. Counter of false secret codes already at 3
207	Cardholder in black list (when card status=3)

208	Card not arrived. Card stolen. Unauthorized use. Fraud suspicion, Card lost
210	Inconsistency of validity date with the cardholders files in track or chip reading mode. Invalid CVV.
380	OK with exceeding
381	OK with capital rising
382	OK NPAI
385	Partial authorization

Array 7 : Response codes from the Finaref authorization center

12.1.4 Buyster

CODE	MEANING
12	Invalid parameter
17	Cancellation from cardholder
24	Impossible operation
25	Unknown transaction
3	Unknown payment recipient
30	Mandatory parameter is empty
34	Fraud suspicion
40	Requested operation not granted
5	Transaction refused
63	Merchant authentication parameters invalid
75	Number of cardholder authentication attempts exceeded (3 attempts)
94	Transaction reference already used
99	Technical problem with the Buyster server

Array 8 : Response codes from the Buyster authorization center

12.2 HTTP Return codes

The first digit indicates the type of answer. There are 5 different types :

CODE	MEANING
1xx	Information – Request received, being processed
2xx	Request has been successfully received, processed and accepted.
3xx	Redirection
4xx	Client error – The request contains an incorrect syntax or cannot be processed.
5xx	Server error – Server failed to process a correct request.

Tableau 9 : HTTP response codes

For more details and for an complete list of response codes, please refer to the HTTP1.1 protocol norm, called RFC2616.

12.3 CURL error codes

CODE	MEANING
1	Protocol not supported
2	Failure during authentication phase
3	Invalid format of URL
4	Invalid format of URL
5	Proxy resolution not possible
6	Host resolution not possible
7	Connection with Host not possible
22	(HTTP) Page not reached
34	(HTTP) Error in Post method
35	Error in SSL connection
42	Callback cancelled
43	Internal error
44	Internal error
45	Inteface error
47	Too many redirections
51	Incorrect remote SSL certificate
52	Server is not responding
53	SSL cryptographic engine not found
54	Problems in initializing SSL cryptographic engine
55	Error in sending data
56	Error in receiving data
57	Internal error
58	Problem with local certificate
59	Impossible to use the given SSL method

Array 10 : CURL error codes

12.4 Paybox character set

The char set supported by the Paybox applications is shown below. Depending on the application, any character received but not present in the matrix below will be deleted from the request or the request will be rejected:

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

12.5 URL Encoded characters

The array below contains a list of the most frequent special characters that must be URL Encoded if they are present in a URL.

Those characters have to be replaced by the corresponding value in the “URL Encoded” column.

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

12.6 URLs to call and IP addresses

The URLs to start transactions with the standard **Paybox System** service:

PLATFORM	ACCESS URL
Pre-production	https://preprod-tpeweb.paybox.com/cgi/MYchoix_pagepaiement.cgi
Main	https://tpeweb.paybox.com/cgi/MYchoix_pagepaiement.cgi
Backup	https://tpeweb1.paybox.com/cgi/MYchoix_pagepaiement.cgi

The URLs to start transactions with the **Paybox System Light (iFrame)** service:

PLATFORM	ACCESS URL
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

The URLs to start transactions with the **Paybox System Mobile** service:

PLATFORM	ACCESS URL
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

The URLs to **cancel subscriptions**:

PLATFORM	ACCESS URL
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

The incoming IP address is the IP address on which the merchant Web site will connect in order to process the transaction.
The outgoing IP address is the IP address from which the merchant Web site will see the callback URLs coming (calls to the IPN URL for example).

It is important that both incoming and outgoing IP addresses are authorized within the firewalls or network equipments in charge of the security within the merchant network infrastructure.

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 Glossary

12.7.1 3-D Secure

The 3-D Secure protocol has been defined by VISA and MASTERCARD in order to solve problem the problems of payment chargeback.
The 3-D Secure protocol is defined by an authentication phase before the payment, during which the cardholder has to authenticate with a code.
Then, if a cardholder challenges a payment realized on Internet, the merchant has the capability to prove that the cardholder is really the buyer.

Each issuer bank defines an authentication method for its cardholders and then holds the responsibility in case of a payment chargeback.
There is a **transfer of responsibility** from the acquirer bank (bank of the merchant) to the issuer bank (bank of the cardholder).

It is also important that, before to activate the 3-D Secure service, the merchant checks with his bank that the merchant contract provided by his bank allows payments with 3-D Secure option. A standard merchant contract will be helpless in case of chargeback.

Paybox is a technical platform between the merchant and his bank, with which he subscribed a merchant contract. The 3-D Secure activation request can be issued by the merchant of by his bank which can require this activation in case of too many charge-backs.
Paybox should then activate this service and inform the merchant and his bank when it has been done.

Once the 3-D Secure service is activated, not all the payments benefit from the transfer of responsibility (guarantee).
The Merchant Back Office allows the merchant to visualize the status of the 3-D Secure payments with the parameter “**Guarantee**” in the **Log** menu.
More detailed information regarding the cardholder authentication is available
Un détail décrivant le résultat de l’authentification du porteur est également présent sous la mention **Statut Porteur 3D Secure**.

The 3-D Secure protocol is processed in 2 phases :

1 – Paybox checks online with Visa and Mastercard if the card is enrolled in the 3D Secure program
2 – Paybox redirects the cardholder to the authentication page of the issuer bank on which the cardholder has to enter a personal code in order to authenticate himself.

The rules described by Visa and Mastercard concerning the transfer or responsibility (or Guarantee) are based on those messages and phases.
For every payment, Paybox can provide the result of those messages and phases.

For more information, please consult our information sheet : ***[Ref 3] « Introduction to 3DSecure ».***

12.7.2 Encodage URL (url-encodé)

All characters are not allowed in a URL (see below the definition of URL). URL encoding allows to convert some special characters in order to transport them within a URL.
Example: « ! » becomes « %21 », « @ » becomes « %40 »

Some functions exist in most of the coding languages in order to make those conversions. For example, *urlencode()* and *urldecode*() can be used in PHP.

12.7.3 FTP

The FTP (File Transfer Protocol) is a protocol of file transfers which enable the downloading of data selected by the Internet user from one computer to another, as in the customer – server model.

12.7.4 HMAC

HMAC (for Hash-based Message Authentication Code) is a standard protocol (RFC 2104) allowing to check the integrity of a string of data. This protocol is used in the Paybox solutions to control the authenticity of the requests sent by a merchant.

Some functions exist in most of the coding languages in order to calculate a HMAC.

12.7.5 HTTP

HTTP (HyperText Transport Protocol) is a protocol used to transfer hypertext or hypermedia documents between a Web server and a Web customer.

12.7.6 IP (IP address)

The IP (Internet Protocol) is the unique address of a computer connected to a network (local network or World Wide Web).

12.7.7 SSL

The SSL (Secure Sockets Layer) protocol enables the secured transmission of forms within the Web and can therefore be used for on-line financial transactions which necessitate the use of a credit card. A hacker who would “listen “ on this connection could not read the data.

12.7.8 URL

The URL (Uniform Resource Locators) are resource addresses on the Internet. A resource can be an http server, a file on your disc, a picture etc.

Example: `http://www.maboutique.com/site/bienvenue.html`