

# PAYBOX DIRECT / PAYBOX DIRECT PLUS

## Integration Manual

Version 8.1

---

**Verifone**<sup>®</sup>

**Verifone**  
11 A, Rue Jacques Cartier, 78 280 Guyancourt, FRANCE

## CHANGE REVIEW

DATE	VERSION	DESCRIPTION	AUTEUR
2015-10-23	7.0	Second method for the 3-D Secure authentications via the product RemoteMPI	M. THOMAS
2018-08-01	8.1	§9.4: update incoming IP addresses. New field URL_ENCODE. §9.5.7: new example using 3-D Secure Variables.	Project Services

## REFERENCES DOCUMENTS

Most of the documents referenced below can be downloaded from our website:

[www.paybox.com](http://www.paybox.com):

REF.	DOCUMENT	DESCRIPTION
Ref 1	ManuellIntegrationVerifone_PayboxSystem_V8.0_EN.pdf	Integration guide for Paybox System.
Ref 2	ParamètresTestVerifone_Paybox_V8.0_EN.pdf	Manual explaining the test environment and the test accounts (pre-production).
Ref 3	GUIDE_UTILISATEUR_BACK_OFFICE_COM_MERCANT_PAYBOX.doc	User guide for the merchant back-office
Ref 4	PAYBOX Fiche présentation 3DSecure.pdf	Product information on 3D secure and advantages for the merchant.
Ref 5	ManuellIntegrationVerifone_RemoteMPI_V8.0_EN.pdf	Integration guide for the remote MPI in order to use 3D secure on the Paybox Direct interface.

## LEGENDE

Following conventions apply in this document:

**Information insert:** content allows a better understanding of the document.

**Warning insert:** content must be read thoroughly.

## WARNING

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

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 & ASSISTANCE

For any merchant or integrator who needs some commercial information, or some technical information or support during the integration process, Verifone Sales service and Technical and client Helpdesk are available:

### Technical and client Helpdesk

Monday - Friday 9h - 18h

[support-paybox@verifone.com](mailto:support-paybox@verifone.com)

**+33 825 305 004** Service 0,15 € / min  
+ prix appel

For any contact with our Sales service or Technical and client Helpdesk, you must provide the following Verifone identifiers:

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

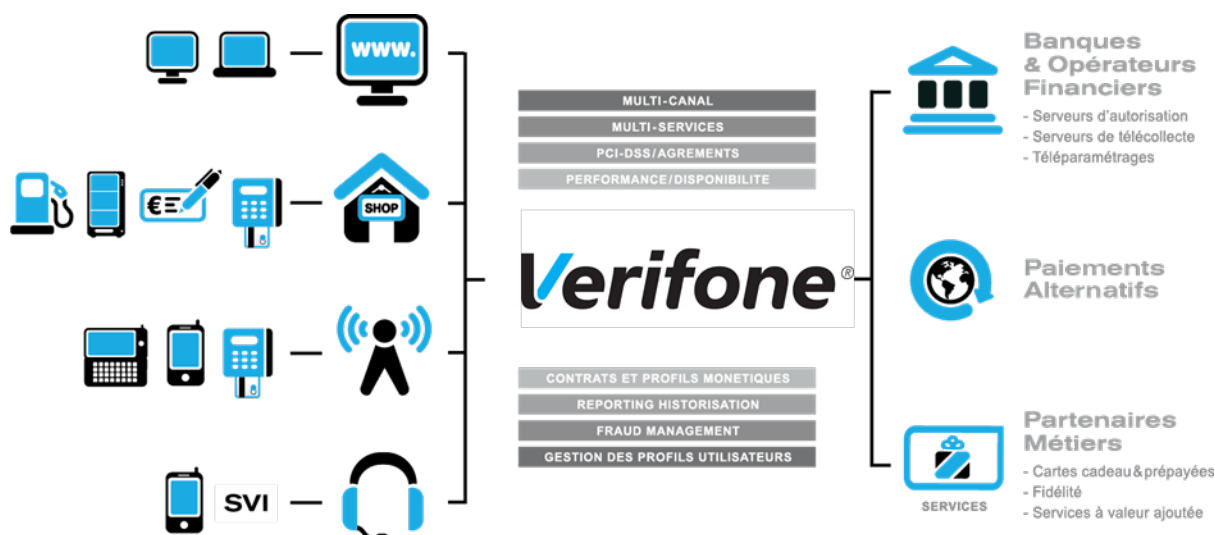
# SUMMARY

<b>CHANGE REVIEW</b> .....	<b>2</b>
<b>REFERENCES DOCUMENTS</b> .....	<b>3</b>
<b>LEGENDE</b> .....	<b>3</b>
<b>WARNING</b> .....	<b>4</b>
<b>INFORMATION &amp; ASSISTANCE</b> .....	<b>4</b>
<b>SUMMARY</b> .....	<b>5</b>
<b>1. INTRODUCTION</b> .....	<b>7</b>
<b>2. PURPOSE OF THIS DOCUMENT</b> .....	<b>8</b>
<b>3. PRÉSENTATION OF THE PRODUCT « PAYBOX DIRECT »</b> .....	<b>9</b>
<b>3.1 HIGH LEVEL DESCRIPTION</b> .....	<b>9</b>
<b>3.2 LIST OF PAYMENT METHODS</b> .....	<b>9</b>
<b>3.3 SECURITY</b> .....	<b>10</b>
<b>4. PROTOCOL DESCRIPTION</b> .....	<b>11</b>
<b>4.1 REQUEST</b> .....	<b>11</b>
<b>4.2 RESPONSE</b> .....	<b>11</b>
<b>4.3 PAYBOX DIRECT PLUS (SUBSCRIPTION MANAGEMENT)</b> .....	<b>13</b>
<b>5. MERCHANT BACK OFFICE</b> .....	<b>15</b>
<b>5.1 ACCESS AND FUNCTIONALITIES</b> .....	<b>15</b>
<b>6. HELPDESK - CONTACT</b> .....	<b>16</b>
<b>6.1 INFORMATION &amp; ASSISTANCE</b> .....	<b>16</b>
<b>6.2 MERCHANT SUBSCRIPTION PROCEDURE</b> .....	<b>16</b>
<b>7. TEST ENVIRONMENT</b> .....	<b>17</b>
<b>8. DATA DICTIONARY</b> .....	<b>18</b>
<b>8.1 PARAMETERS USED IN A PAYBOX DIRECT / PAYBOX DIRECT PLUS CALL20</b>	
<b>8.2 RETURN PARAMETERS PAYBOX DIRECT / PAYBOX DIRECT PLUS..</b>	<b>30</b>

<b>9.</b>	<b>APPENDIX .....</b>	<b>35</b>
9.1	RETURN CODES FROM THE AUTHORIZATION CENTER.....	35
9.2	PAYBOX CHARACTER SET .....	39
9.3	URL ENCODING CHARACTERS .....	40
9.4	URL AND IP ADDRESSES TO CALL.....	41
9.5	EXAMPLES OF REQUESTS/RESPONSE MESSAGES FOR PAYBOX DIRECT.....	41
9.6	GLOSSARY.....	47

# 1. INTRODUCTION

Verifone 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 an Omni-channel and multi-services centralized platform:

- **Omni-channel** : the Verifone 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 Verifone 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, Verifone 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 Verifone. 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. PRÉSENTATION OF THE PRODUCT « PAYBOX DIRECT »

### 3.1 HIGH LEVEL DESCRIPTION

The product « Paybox Direct PPPS » (Paybox Payment Per Socket) allows to transmit a payment request using a HTTPS «request» and to receive in the same HTTPS session a response that provides real-time information on the outcome of the request: accepted or rejected.

The mechanism is very simple:

- Create a HTTPS « request »,
- Call the right URL on the Paybox servers,
- Wait for the HTTPS answer in the same sessions returned by Paybox after the request was processed.

### 3.2 LIST OF PAYMENT METHODS

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

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	
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
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 Verifone platform using different information fields:

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

These identification parameters are provided by Verifone when the registration of the Merchant is confirmed.

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

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

## 4. PROTOCOL DESCRIPTION

### 4.1 REQUEST

The messages are always constructed by concatenating multiple couples of a parameter with a value. (... TYPE=00001&MONTANT=1000&SITE=1999888&...) similar to the mechanism used in a HTML form for posting values to a webserver. Mind that the GET method is not supported when calling the Paybox Direct applications.

To carry out a 3D-Secure transaction, merchants will need to authenticate the cardholder before calling the Paybox Direct applications.

This authentication can be performed using the Remote MPI product provided by Verifone. Remote MPI usage is described in document **[Ref 5] Manuel Integration Paybox Remote MPI**.

The request is transmitted to the Paybox servers using the request URL mentioned for the Paybox Direct service (see **§9.4 URL d'appel et Adresses IP**).

In case the answer contains any of the error codes "00001", "00097", or "00098", it is recommended to call the URL of the secondary server of Paybox Direct (see the same chapter for more information).

In order to obtain an answer from the Verifone servers, the parameter "SITE" and "RANG" must contain the correct values.

### 4.2 RESPONSE

**Warning:** Response can take as long as 40 seconds since a bank is allowed up to 30 seconds to answer an authorization request.

The response follows the same format as the request and a series of variables is returned in the HTTP answer.

The parameters SITE, RANG and NUMQUESTION are always echoed from the request and allows the receiving process to correctly identify to what request corresponds the answer. It is advised to verify those values.

Paybox Direct also returns a parameter "CORESPONSE" that allows to see if the call was successfully processed or not. The value 00000 indicates a correct processing of the request.

In case of an error the parameter "COMMENTAIRE" contains a detailed error message.

In case of any problems, those 2 variables allow for a correct diagnosis, the support service of Verifone might request those values when you ask for their help.

## Example using an HTML form:

```

<html ><body>

<form action="https://preprod-ppps.paybox.com/PPPS.php" method="post" name="Tests Paybox
Direct">

    Date (JJMMAAAA)
    <input name="DATEQ" value="20032007" size="8" maxlength="8" type="text"><br>

    Type de question
    <input name="TYPE" value="00001" size="5" maxlength="5" type="text"><br>

    Numero de question
    <input name="NUMQUESTION" value="0000000001" size="10" maxlength="10" type="text"><br>

    Montant
    <input name="MONTANT" value="1000" size="10" maxlength="10" type="text"><br>

    Site
    <input name="SITE" value="1999888" size="7" maxlength="7" type="text"><br>

    Rang
    <input name="RANG" value="99" size="2" maxlength="2" type="text"><br>

    Reference commande
    <input name="REFERENCE" value="Hello World" size="30" maxlength="30" type="text"><br>

    <input name="VERSION" value="00104" type="hidden"><br>
    <input name="CLE" value="19998881" type="hidden"><br>
    <input name="IDENTIFIANT" value="" type="hidden"><br>
    <input name="DEVISE" value="978" type="hidden"><br>
    <input name="PORTEUR" value="1111222233334444" type="hidden"><br>
    <input name="DATEVAL" value="1010" type="hidden"><br>
    <input name="CVV" value="123" type="hidden"><br>
    <input name="ACTIVITE" value="024" type="hidden"><br>
    <input name="ARCHIVAGE" value="AXZ130968CT2" type="hidden"><br>
    <input name="DIFFERE" value="000" type="hidden"><br>
    <input name="NUMAPPEL" value="" type="hidden"><br>
    <input name="NUMTRANS" value="" type="hidden"><br>
    <input name="AUTORISATION" value="" type="hidden"><br>
    <input name="PAYS" value="" type="hidden"><br>

<input type="submit">

</form>

</body></html>

```

## 4.3 PAYBOX DIRECT PLUS (SUBSCRIPTION MANAGEMENT)

### 4.3.1 The Principle

When the merchant wants to register a new subscriber on the Paybox Direct Plus Platform, all the same parameters as used for an authorization request need to be submitted and in addition a unique subscriber number must be added to the message.

Verifone will then verify if the subscriber number is unique and will perform several checks (expiration of the card, black list,). If all the checks are successful an authorization-only message (without debit) will be sent to the acquirer and if the transaction is approved by the acquirer the subscriber will be registered on the platform. A part of the PAN (card number) will be stored on the Verifone platform and the other part will be return to the merchant in order for him to store this information together with the subscriber number and the validity of the card.

The same mechanism is used in case of a modification of a previously registered subscriber.

For debit, credit, refund or cancellation of a previously registered subscription, the merchant will have to provide the subscriber number, the part of the PAN in his possession and the validity of the card together with other mandatory fields in the “Paybox Direct” protocol.

### 4.3.2 How it works

For all the requests of the type: 51, 52, 53, 54, 55, 57 and 58 a previous registration of the subscriber is mandatory. A registration is done with a request of type 56 towards the Verifone server.

The request for creation of a new subscriber will automatically result in an authorization message being sent to the acquirer for the exact amount as specified in the request in order to validate the card. In case the authorization is accepted by the acquirer the subscriber will be created in the database of Paybox, but a rejection by the acquirer will result in the subscriber not being registered.

If the creation of the subscriber was successful a request of type 52 (debit) on the subscriber can be sent for the amount previously authorized. If the amount required is different from the amount specified in the creation of the subscriber, a message of the type 53 should be sent in order to authorize the desired amount and a message 52 with the desired amount to be debited.

**Information:** Two authorization requests send in quick succession can trigger a refusal from the bank.  
It is recommended to allow intervals between a subscriber registration (56) and message of the type (51) and (53).

It is also possible to create a new subscriber using the Paybox System (redirect payment page). In order to make this work, the subscriber reference needs to be requested (Field 'U'

in the PBX\_RETOUT). The response message from Verifone will then contain 3 data elements: Part of the PAN (card number used), Expiry data of the card and the CVV. The first two data elements need to be stored for future use when calling Paybox Direct Plus.

For more detailed information on how to do this, please read the integration guide for Paybox System.

## 5. MERCHANT BACK OFFICE

Once the merchant has been registered within Verifone, 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 ...).

### 5.1 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 3] Guide Utilisateur du Back Office**: <http://www1.paybox.com/espace-integrateur-documentation/manuels/?lang=en>

## 6. HELPDESK - CONTACT

### 6.1 INFORMATION & ASSSITANCE

For any merchant or integrator who needs some commercial information, or some technical information or support during the integration process, Verifone Sales service and Technical and client Helpdesk are available:

#### Technical and client Helpdesk

Monday - Friday 9h - 18h

[support-paybox@verifone.com](mailto:support-paybox@verifone.com)

**+33 825 305 004** Service 0,15 € / min  
+ prix appel

For any contact with our Sales service or Technical and client Helpdesk, you must provide the following Verifone identifiers:

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

The functions of the Technical and client Helpdesk 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

### 6.2 MERCHANT SUBSCRIPTION PROCEDURE

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

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

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

## 7. TEST ENVIRONMENT

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

Verifone 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 **[Ref2]** « **Parametres\_Test\_Verifone\_Paybox\_V8.0\_FR.pdf** » available for download here:

<http://www1.paybox.com/espace-integrateur-documentation/manuels/?lang=en>

## 8. DATA DICTIONARY

All possible parameters for the Paybox Direct and Paybox Direct Plus interface are listed in the following table. The following pages explain every individual parameter in detail (format, content, examples).

VARIABLE	REQUEST	RESPONSE	DESCRIPTION
ACQUEREUR	X		Payment method to be used
ACTIVITE	X		Call origin
ARCHIVAGE	X		Reference for archiving
AUTORISATION	X	X	Authorization number If present in the request message, an authorization was obtained by telephone.
CODEREPOSE		X	Response code giving more detail of the status of the request : request accepted or rejected [see below for more detail on the various possibilities].
COMMENTAIRE		X	Information filed (e.g. : error message)
CVV	X		Visual cryptogram of the card
DATENAISS	X		Specific to COFINOGA
DATEQ	X		Date and time of the request
DATEVAL	X		Expiry date of the card
DEVISE	X		Currency
DIFFERE	X		Number of days for a postponed settlement
ERRORCODETEST	X		Error message to be returned (forced for test purposes)
ID3D	X		3D-Secure context returned by the remote MPI. This variable must be populated if before you carried out Secure authentication via the product RemoteMPI. If you prefer do not use the context ID3D, you need use the following variables sent by the product RemoteMPI : 3DSTATUS, 3DENROLLED, 3DECI, 3DERROR, 3DXID, 3DCAVV, 3DCAVVALGO and 3DSIGNVAL
3DCAVV	X		Sent by ACS
3DCAVVALGO	X		ID of algorithm during the authentication of the cardholder
3DECI	X		E-Commerce Indicator
3DENROLLED	X		Status of the 3D Secure enrolment of the cardholder
3DERROR	X		Error sent by MPI

3DSIGNVAL	X		Status of the electronic signature
3DSTATUS	X		Status of the authentication of the cardholder
3DXID	X		Reference from the MPI
MONTANT	X		Amount
NUMAPPEL	X	X	Call number returned by Paybox
NUMQUESTION	X	X	Unique sequential number
NUMTRANS	X	X	Transaction number assigned by Paybox
PAYS	X	X	Country code of the issuance of the card
PORTEUR	X	X	PAN number of the card
PRIV_CODETRAITEMENT	X		Specific to SOFINCO/COFINOGA
RANG	X	X	Rang number of the merchant
REFABONNE	X	X	Reference of a stored card number (Direct Plus)
REFERENCE	X		Transaction reference number
REMISE		X	Paybox identifier of the settlement file
SHA-1	X	X	Indicator that a hash on the card number needs to be returned.
SITE	X	X	Site number of the merchant
STATUS		X	Status of the transaction
TYPE	X		Type of action requested
TYPECARTE	X	X	Type of card
URL_ENCODE	X		Value send will be url-decoded before
VERSION	X		Version of the protocol used

**Table 1: Overview of all Paybox Direct and Paybox Direct Plus parameters**

## 8.1 PARAMETERS USED IN A PAYBOX DIRECT / PAYBOX DIRECT PLUS CALL

### 8.1.1 SITE

Format: 7 digits. **Mandatory**.

This is the site number (POS) typically provided by the bank to the merchant. Outside France this number is assigned to the Merchant by Verifone.

Example: 1999888

### 8.1.2 RANG

Format: 2 digits. **Mandatory**.

This is the rank number (or « machine ») provided by the bank to the merchant. Outside France this number is assigned to the Merchant by Verifone.

Example: 01

### 8.1.3 VERSION

Format: 5 digits. **Mandatory**.

Version of the protocol PPS used.

Example: 00103 for Paybox Direct / 00104 for Paybox Direct Plus

### 8.1.4 TYPE

Format: 5 digits. **Mandatory**.

Paybox Direct and Paybox Direct Plus support various types of operations on a transaction that allow to manage the life-cycle of a transaction (authorization, capture, cancel, refund, etc.).

This parameter defines the action that is requested.

In case of a capture (00002) following a previous authorization request, it is strongly recommended:

- To wait a little moment (a few seconds) between sending the request for authorization and sending in the capture.

- To send the capture to the same platform (Nanterre or Strasbourg) where the authorization was sent, in order to avoid problems with replication between the two production platforms.

CODE	DESCRIPTION	OPTION
00001	Authorization only	
00002	Debit (Capture)	
00003	Authorization + Capture	
00004	Credit	
00005	Cancel	
00011	Check if a transaction exists	
00012	Transaction without authorization request	
00014	Refund	
00017	Inquiry	
00051	Authorization only on a subscriber	Only Direct Plus
00052	Debit on a subscriber	Only Direct Plus
00053	Authorization + Capture on a subscriber	Only Direct Plus
00054	Credit on a subscriber	Only Direct Plus
00055	Cancel of a transaction on a subscriber	Only Direct Plus
00056	Register new subscriber	Only Direct Plus
00057	Update an existing subscriber	Only Direct Plus
00058	Delete a subscriber	Only Direct Plus
00061	Authorization only	Only Direct Plus

**Table 2: PAYBOX DIRECT question type list**

### 8.1.5 DATEQ

Format: 14 digits. **Mandatory.**

Date and time of the request using the format DDMMYYYYHHMMSS. (day month year hour minute seconds).

Used in the SQL queries for the request of type 11 (format JJMMAAAA)

Example: 13042016125959

### 8.1.6 NUMQUESTION

Format : 10 digits (min :1 ; max : 2147483647). **Mandatory.**

Unique identifier for the request that allows to avoid confusion in case of multiple simultaneous requests.

Every request needs to have a unique value for NUMQUESTION for a certain day. The value can be reset/reused the next day.

Example: 0000000001

### 8.1.7 CLE

Format: 8 à 10 characters. **Mandatory.**

This field allows to authenticate the originator of the request and allows for additional security for the PPPS exchange of messages.

The value for this parameter corresponds to the password for the merchant back-office that is provided by the technical support upon the creation of the merchant account on the Paybox platform.

Starting October 2013, passwords sent by Paybox always have a length of 10 characters

### 8.1.8 MONTANT

Format: 10 digits. **Mandatory for requests of type 1, 2, 3, 4, 5, 11, 12, 14, 51, 52, 53, 54, 55, 56, 57, 61.**

Amount of the transaction in cents (no decimal point).

Example: for 19€90 / 0000001990

## 8.1.9 DEVISE

**Format:** 3 digits. **Mandatory for requests of type 1, 2, 3, 4, 5, 11, 12, 14, 51, 52, 53, 54, 55, 56, 57, 61.**

Currency code for the transaction according to ISO 4217 (numeric code)

Examples: Euro: 978 / US Dollar: 840 / CFA: 952

Before issuing transaction in foreign currencies make sure that your merchant contract allow you to do and that your account is correctly configured.

## 8.1.10 REFERENCE

**Format:** 1 à 250 characters. **Mandatory for requests of type 1, 2, 3, 4, 5, 11, 12, 51, 52, 53, 54, 55, 56, 61.**

This is the merchant order reference (free field). This allows the merchant to link his platform to the Paybox platform using a reference number.

Example: CMD9542124-01A5G

## 8.1.11 REFABONNE

**Format:** 1 à 250 characters. **Mandatory for requests of type 51, 52, 53, 54, 55, 56, 57, 58, 61.**

Merchant reference number allowing him to clearly identify the subscriber (profile) that corresponds to the transaction.

Example: AZERTY1234567

## 8.1.12 PORTEUR

**Format:** up to 19 characters. **Mandatory for requests of type 1, 3, 4, 12, 51, 53, 54, 55, 56, 57, 61.**

PAN (card number) of the customer, without any spaces and left aligned (Type 1, 3, 4, 12, 56 and 57).

Subscriber number for the request. Empty (binary zeros) in the context without subscription (Type 51, 53, 54 and 55).

Example: 1111222233334444

### 8.1.13 DATEVAL

**Format:** Date (MMYY) **Mandatory for requests of type 1, 3, 4, 12, 51, 53, 54, 55, 56, 57, 61.**

Expiry date of the card.

Example: 1216 (décembre 2016)

### 8.1.14 CVV

**Format:** 3 or 4 characters.

Visual cryptogram on the back of the card.

Remark: The card of AMERICAN EXPRESS have on the front of the card a CIN (Card Identification Number) containing 4 digits.

Example: 123

### 8.1.15 ACTIVITE

**Format:** 3 digits.

**Valeur par défaut:** 024

This parameter allows to inform the acquirer (bank) how the transaction was initiated and how the card entry was realized.

The following values are supported for the card entry mode:

CODE	DESCRIPTION
020	Not specified
021	Telephone order
022	Mail order
023	Minitel (France)
024	Internet payment
027	Recurring payment



## 8.1.16 ARCHIVAGE

Format: up to 12 alphanumeric characters

This reference is transmitted to the acquirer (bank) of the merchant during the settlement of the transaction. The reference needs to be unique and allows the merchant to inquire for additional information from the acquirer (bank) in case of a dispute.

## 8.1.17 DIFFERE

Format: maximum 3 digits

Number of days to postpone the settlement.

In the back-office it is possible to remove the delay and submit the transaction for settlement to the acquirer (bank).

For Example, a transaction that was done on the 2nd of November, and postponed for settlement on the 4th of November, can be unblocked in the back-office manually.

A default value can be configured on the subscription form and the opening of the merchant account. If the parameter is set in the transaction, this value overrides the default value of the merchant.

Example: 004 pour gérer un différé de 4 jours

## 8.1.18 NUMAPPEL

Format: 10 digits. **Mandatory for requests of type 2, 5, 14, 52, 55.**

This number is returned by Verifone when a transaction is successfully processed.  
For Paybox System, the parameter is returned in the return post (IPN)  
For Paybox Direct, the parameter is always present in the response.  
The parameter can also be seen in the merchant back-office.

## 8.1.19 NUMTRANS

Format: 10 digits. **Mandatory for requests of type 2, 5, 14, 17, 52, 55.**

This number is returned by Verifone when a transaction is successfully processed.  
For Paybox System, the parameter is returned in the return post (IPN)  
For Paybox Direct, the parameter is always present in the response.  
The parameter can also be seen in the merchant back-office.

## 8.1.20 AUTORISATION

Format: up to 10 characters. Can be used in the requests of type 1, 3, 51, 56 et 57

Authorization number provided by the merchant that was obtained by telephone call to the acquirer (bank)

Example: 123456

## 8.1.21 PAYS

Format: empty.

If the parameter is present (even empty), Paybox Direct returns the country code of issuance of the card in the response.

## 8.1.22 PRIV\_CODETRAITEMENT

Format: 3 digits.

Parameter filled in by the merchant to indicate the payment option that is proposed to the cardholder of a SOFINCO card (or partner card of SOFINCO) or COFINOGA.

## 8.1.23 DATENAISS

Format: Date DDMMYYYY (8 digits).

Birthday of the cardholder for the cards of COFINOGA.

## 8.1.24 ACQUEREUR

Format: up to 16 characters.

Defines the payment method used. The possible values are:

- PAYPAL
- EMS
- ATOSBE
- BCMC
- EQUENS
- PSC
- FINAREF

- 34ONEY

If the request does not involve one the mentioned acquirers, the parameter can be left empty.

### 8.1.25 TYPECARTE

Format: empty

If the parameter is present (even empty), Paybox Direct will return the type of card in the response (for a payment using with a card).

### 8.1.26 URL\_ENCODE

Format: 1 character

If the parameter contains O, Paybox Direct will URL-decode the value provided in each field before evaluating them.

Example: O

### 8.1.27 SHA-1

Format: 40 question mark.

If the parameter is present (even empty), Paybox Direct will return the hash of the card in the response (for a payment with a card).

The algorithm used to hash the card number is SHA-1.

Example: ???

### 8.1.28 ERRORCODETEST

Format: 5 digits

The error code to return (forced) while doing integration testing in the pre-production environment. In production the parameter is not taken into account.

### 8.1.29 ID3D

Format: 20 digits

Context identifier Verifone that holds the authentication result of the MPI (see the document « PAYBOX RemoteMPI English.doc »)

This authentication context is stored during 5 minutes.

After that period, the Paybox applications consider the authentication phase of the cardholder invalid due to a time-out.

This variable must be used if you want use the context returned by the RemoteMPI product. If you need to not have this constraint of 5 minutes, but lose an facility of integration, you can use instead of the 8 following variables: 3DSTATUS, 3DENROLLED, 3DECI, 3DERROR, 3DXID, 3DCAVV, 3DCAVVALGO and 3DSIGNVAL.

Warning these variables must not be URL encoded.

For an example using these variables, see **§9.5.7 Call using 3-D Secure variables (Remote MPI)**

### 8.1.30 3DCAVV

Format: 28 characters.

Sent by ACS. Base64 encoding.

This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D. This variable must not be URL-encoded when calling Paybox Direct.

Example: jNEEdZ7c5MThARFVdvTZKmZSAUc=

### 8.1.31 3DCAVVALGO

Format: up to 64 characters

ID of algorithm during the authentication of the cardholder.

This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D.

Example: 0000000001

### 8.1.32 3DECI

Format: 2 digits

E-Commerce Indicator. Level of the securisation of the authentication

This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D.

### 8.1.33 3DENROLLED

Format: 1 character

Status of the 3-D Secure enrolment of the cardholder.  
This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D.

Possible values :

- Y : Cardholder enroled
- N : Cardholder not enroled
- U : Error

### 8.1.34 3DERROR

Format: up to 6 characters

Error sent by the MPI  
This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D.

### 8.1.35 3DSIGNAL

Format: 1 character.

Status of the electronic signature.  
This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D.

Possible values: Y or N

### 8.1.36 3DSTATUS

Format: 1 character.

Status of the 3-D Secure authentication of the cardholder.  
This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D.

Possible values:

- Y: Cardholder full authenticated

- N: Cardholder not authenticated
- A: Forcing authentication by the bank of the cardholder.
- U: Technical error during authentication of the cardholder

### 8.1.37 3DXID

Format: up to 28 characters

Reference form the MPI. Base64 encoding.

This variable must be sent to the product interfaces Paybox Direct if you never use the context-based solution ID3D. This variable must not be URL-encoded when calling Paybox Direct

Example: IC8wIK1CVDB2b4w9Hme63bmz/w4=

## 8.2 RETURN PARAMETERS PAYBOX DIRECT / PAYBOX DIRECT PLUS

### 8.2.1 SITE

Format: 7 digits.

This is the site number (POS) typically provided by the bank to the merchant. Outside France this number is assigned to the Merchant by Verifone. Echo from the parameter in the request.

Example: 1999888

### 8.2.2 RANG

Format: 2 digits.

This is the rang number (or « machine ») provided by the bank to the merchant. Outside France this number is assigned to the Merchant by Verifone. Echo from the parameter in the request.

Example: 01

### 8.2.3 NUMQUESTION

Format: 10 digits (min: 1 ; max: 2147483647).

Unique identifier for the request that allows to avoid confusion in case of multiple simultaneous requests.

Every request needs to have a unique value for NUMQUESTION for a certain day.

The value can be reset/reused the next day.  
Echoed from the parameter in the request.

Example: 0000000001

## 8.2.4 NUMAPPEL

Format: 10 digits

Number of the request generated on the Verifone platform.

Example: 0000782653

## 8.2.5 NUMTRANS

Format: 10 digits

Number of the transaction generated on the Verifone platform..

Example: 0000563149

## 8.2.6 AUTORISATION

Format: up to 10 characters maximum (most commonly 6 digits)

Authorization number delivered by the authorization system of the acquirer of the merchant, only if the transaction was accepted.

Example: 168753

## 8.2.7 CODEREPOSE

Format: 5 digits

Response code with the status of the request processed: request accepted or rejected.

CODE	DESCRIPTION
00000	Operation successful.
00001	The connection to the authorization center has failed or an internal error has been produced. It is recommended to try the transaction again on the secondary data center: ppps1.paybox.com.
001xx	The payment was rejected by the authorization center. [see <b>§9.1 Return codes from the authorization center</b> ].

	In case of a successful authorization by the authorization center of the acquirer (bank), this field will be filled in with “00000”.
00002	Error due to incoherence.
00003	Internal error Paybox. In this case it is advised to use the secondary datacenter: ppps1.paybox.com.
00004	Cardholder number invalid.
00005	Request number invalid. (NUMQUESTION)
00006	Access refused or combination site / rang not correct.
00007	Date invalid.
00008	Expiry data not correct.
00009	Type of requested operation invalid.
00010	Unknown currency.
00011	Amount not correct.
00012	Order reference invalid.
00013	This version is no longer supported.
00014	Received request incoherent.
00015	Error accessing data previously referenced.
00016	This subscriber already exists (when creating a new subscriber).
00017	The subscriber does not exist.
00018	Transaction was not found (request type 11).
00019	Reserved.
00020	Visual cryptogram missing.
00021	Card not authorized.
00022	Threshold reached
00023	Cardholder already seen
00024	Country code filtered
00026	Activity code incorrect.
00040	Cardholder enrolled but not authenticated
00097	Connection timeout
00098	Internal connection timeout
00099	Incoherence between query and reply.

**Table 3: PAYBOX DIRECT response code list**

Example: 00007 (date invalid)



## 8.2.8 REFABONNE

Format: up to 250 characters

Subscriber number for the request. Empty (binary zeros) in the context without subscription.

Example: AZERTY1234567

## 8.2.9 PORTEUR

Format: up to 19 characters

Part of the card number returned by Verifone upon creation or modification of a subscriber. In other cases equal to the field in the request.

Example: 1111222233334444

## 8.2.10 COMMENTAIRE

Format: up to 100 characters

Descriptive message with information (typical descriptive message when an error occurs).

Example: PAYBOX+PPPS

## 8.2.11 PAYS

Format: 3 characters (alphabetic code ISO3166 )

Country code of issuance of the card. The value «???» is returned if the country is unknown.

Example: FRA

## 8.2.12 TYPECARTE

Format: up to 10 characters

Type of card used for the payment

Example: VISA

### 8.2.13 SHA-1

Format: 40 characters (SHA-1 encoded in hexadecimal)

SHA-1 hash on the PAN (card number) used in the payment.

Example: F8BF2903A1149E682BE599C5C20788788256AA46

### 8.2.14 STATUS

Format: up to 32 characters

Only provided in case of a request of type 17.

Status of the transaction. The possible values are:

- Remboursé, (refunded)
- Annulé, (cancelled)
- Autorisé, (authorised)
- Capturé, (captured)
- Crédit, (credit)
- Refusé, (rejected)
- Demande de solde (Carte cadeaux), (balance inquiry) (gift cards)
- Crédit Annulé, (credit cancelled)
- Rejet support (rejected)

The text between brackets is only for information purposes.

### 8.2.15 REMISE

Format: up to 9 digits.

Only returned in case of a request of type 17.

Paybox identifier of the settlement file.

Example: 509625890

## 9. APPENDIX

### 9.1 RETURN CODES FROM THE AUTHORIZATION CENTER

This information is returned in the response message.

See §8.2.7 CODEREPOSE.

#### 9.1.1 CB (Carte Bancaire) network, Acquirer, American Express

CODE	DESCRIPTION OF THE RESPONSE CODE
00	Transaction accepted or successfully processed
01	Contact the issuer of the card
02	Contact the issuer of the card
03	Invalid merchant
04	Keep the card
05	Do not honor
07	Keep the card, special conditions
08	Authorized after identification of the cardholder
12	Invalid transaction
13	Invalid amount
14	Invalid PAN (card number)
15	Unknown issuer
17	Cancellation by customer
19	Please retry later
20	Error in answer (error in domain server)
24	Update file not supported
25	Unable to find data in file
26	Duplicate record, previous record updated

27	Error when editing field while updating file
28	Access denied on file
29	Update file not possible
30	Error in format
31	Acquirer ID unknown
33	Expired card
34	Fraud suspicion
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 acceptor 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.
98	server unreachable (put by the server)
99	Incident initiating domain.

Table 4: Response codes of card authorization network

### 9.1.2 Cetelem/Aurore and Rive Gauche network

CODE	DESCRIPTION OF THE RESPONSE CODE
00	Transaction accepted or successfully processed
01	Wrong or unknown merchant number
02	Card number incorrect
03	Wrong birthday or secret code
04	Card cannot be funded
05	Problem with server CETELEM
06	Unknown card
07	Amount requested rejected
08	Card expired
09	Card not compatible with merchant
10	Unknown
11	Rejected
12	Wrong currency code
13	Reference of transaction missing
14	Amount of the transaction incorrect
15	Payment terms incorrect
16	Meaning of the transaction incorrect
17	Payment terms incorrect

Table 5: Response codes from the authorization center of Cetelem

### 9.1.3 Finaref network

CODE	DESCRIPTION OF THE RESPONSE CODE
000	OK
101	Card expired. Cardholder validity expired.
103	Unknown merchant. Unknown merchant identifier.
110	Incorrect amount
111	Account/cardholder unknown
115	Service not available. Zero ceiling. Function/processing code unknown
116	Insufficient funds
117	1 <sup>st</sup> or 2 <sup>nd</sup> code wrong
119	Cardholder or account status is blocked. Cardholder or account status is invalid. Card blocked.
120	Invalid merchant. Invalid currency code. Account not authorized. Invalid or unknown commercial operation.
121	Insufficient funds
125	Card not active
126	Secret code missing. Format error in start date security information.
128	Error while checking history of wrong codes
129	CVV2 incorrect
183	Account / Cardholder invalid
184	Incoherence of validity date with file cardholder manual entry
188	Entry mode invalid. Identification equipment incoherent.
196	Problem while accessing file
206	3r attempt secret code failed. Wrong attempts counter already 3.
207	Cardholder blocked (while card status=3)
208	Card not received. Card stolen. Abuse. Fraud suspicion, Card lost

210	Incoherence of validity date with file cardholders magnetic stripe or chip. Wrong CVV
380	OK with overdraft
381	OK with capital increase
382	OK NPAI
385	Partial Authorization

Tableau 6 : Response codes for authorization center Finaref

## 9.2 PAYBOX CHARACTER SET

The following table indicates the character set supported by Verifone. Any characters other than those mentioned in the table will be deleted by the application or the request will be rejected:

0	\0	\t	\n	\r
1				
2	!	"	#	\$ % & ( ) * + , - . /
3	0	1	2	3 4 5 6 7 8 9 : ; < = > ?
4	@	A	B	C D E F G H I J K L M N O
5	P	Q	R	S T U V W X Y Z [ \ ] ^ _
6	`	a	b	c d e f g h i j k l m n o
7	p	q	r	s t u v w x y z {   } ~
8				
9				
A	i	¡	«	
B			»	¿
C	À	Á	Â	Ã Ä Å Æ Ç È É Ê Ë Ì Í Î 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 ñ ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

## 9.3 URL ENCODING CHARACTERS

The following table contains the most commonly used special characters in the left column and their corresponding encoding to be used when submitting those special characters in an URL.

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



## 9.4 URL AND IP ADDRESSES TO CALL

In order to use the Paybox Direct service:

SITE	URL TO CALL
<b>Pre-production</b>	https://preprod-ppps.paybox.com/PPPS.php
<b>Main</b>	https://ppps.paybox.com/PPPS.php
<b>Secondary</b>	https://ppps1.paybox.com/PPPS.php

**The incoming IP address** is the address to be called by the merchant's server to request a transaction.

**The outgoing IP address** is the address that the merchant's server will see when receiving information at the end of a call (call back for example).

It is important that those IP addresses are correctly configured and allowed on the infrastructure of the merchant in order to allow outgoing and incoming traffic, especially if IP filtering and/or firewall equipment is in place.

PLATE-FORME	INCOMING ADDRESS	OUTGOING ADDRESS
<b>Preproduction</b>	195.101.99.73	N/A
	195.101.99.67	
<b>Production</b>	194.2.160.81	N/A
	195.25.67.1	

## 9.5 EXAMPLES OF REQUESTS/RESPONSE MESSAGES FOR PAYBOX DIRECT

Below are examples documented for the most common types of requests using PPPS. Both the request and the response are illustrated.

### 9.5.1 Simple authorisation request

**Request:**

```
VERSION=00104&TYPE=00001&SITE=1999888&RANG=32&CLE=1999888I&NUM
QUESTION=194102418&MONTANT=1000&DEVISE=978&REFERENCE=TestPaybo
```

x&PORTEUR=1111222233334444&DATEVAL=0520&CVV=222&ACTIVITE=024&DATEQ=30012013&PAYS=

**Response:**

NUMTRANS=0001480203&NUMAPPEL=0002269494&NUMQUESTION=0194102418  
&SITE=1999888&RANG=32&AUTORISATION=XXXXXX&CODEREPOSE=00000&COMMENTAIRE=Demande traitée avec  
succès&REFABONNE=&PORTEUR=&PAYS=???

## 9.5.2 Capture

This request allows to « capture » (confirm) the transaction authorized in the above example. In order to reference the transaction you need to use the parameters NUMTRANS and NUMAPPEL (highlighted in yellow).

**Request:**

VERSION=00104&TYPE=00002&SITE=1999888&RANG=32&CLE=1999888I&NUMQUESTION=194102419&MONTANT=1000&DEWISE=978&REFERENCE=TestPaybox&NUMTRANS=0001480203&NUMAPPEL=0002269494&DATEQ=30012013&PAYS=

**Response:**

NUMTRANS=0001480203&NUMAPPEL=0002269494&NUMQUESTION=0194102419  
&SITE=1999888&RANG=32&AUTORISATION=XXXXXX&CODEREPOSE=00000&COMMENTAIRE=Demande traitée avec  
succès&REFABONNE=&PORTEUR=&PAYS=???

## 9.5.3 Refund

**Request:**

VERSION=00104&TYPE=00014&SITE=1999888&RANG=32&CLE=1999888I&NUMQUESTION=194102420&MONTANT=1000&DEWISE=978&REFERENCE=TestPaybox&NUMTRANS=0001480203&NUMAPPEL=0002269494&ACTIVITE=024&DATEQ=30012013&PAYS=

**Response:**

NUMTRANS=0001480204&NUMAPPEL=0002269494&NUMQUESTION=0194102420  
&SITE=1999888&RANG=32&AUTORISATION=XXXXXX&CODEREPOSE=00000&COMMENTAIRE=Demande traitée avec  
succès&REFABONNE=&PORTEUR=&PAYS=???

## 9.5.4 Inquiry

This request allows to inquire the status of a transaction, par exemple to make sure that the status of the transaction on the Paybox platform corresponds with your information system, in case of a time-out or communication problem.

### Request:

```
VERSION=00104&TYPE=00017&SITE=1999888&RANG=32&CLE=1999888I&NUM
QUESTION=194102421&MONTANT=1000&DEVISE=978&REFERENCE=TestPaybo
x&NUMAPPEL=0002269494&NUMTRANS=0001480203&DATEQ=30012013&PAYS=
```

### Response:

```
NUMTRANS=0001480203&NUMAPPEL=0002269494&NUMQUESTION=0194102421
&SITE=1999888&RANG=32&AUTORISATION=XXXXXX&CODEREPOSE=00000&CO
MMENTAIRE=Demande traitée avec
succès&REFABONNE=&PORTEUR=&PAYS=???&STATUS=Remboursé
```

## 9.5.5 Create a new subscriber (register a new card)

This request allows to register a card on the Paybox platform. In the response Paybox will provide a token that can later be used to debit the registered card. This avoids the need to store the card on the merchant's infrastructure.

### Request:

```
VERSION=00104&TYPE=00056&SITE=1999888&RANG=32&CLE=1999888I&NUM
QUESTION=194102422&MONTANT=1000&DEVISE=978&REFERENCE=TestPaybo
x&PORTEUR=1111222233334444&DATEVAL=0520&CVV=222&REFABONNE=ABOD
OCUMENTATION001&ACTIVITE=027&DATEQ=30012013&PAYS=
```

### Response:

```
NUMTRANS=0001480205&NUMAPPEL=0002269498&NUMQUESTION=0194102422
&SITE=1999888&RANG=32&AUTORISATION=XXXXXX&CODEREPOSE=00000&CO
MMENTAIRE=Demande traitée avec
succès&REFABONNE=ABODOCUMENTATION001&PORTEUR=SLDLrCsLMPC&PAYS=
???
```

## 9.5.6 Debit a subscriber

This request allows to debit a previously registered card (subscriber). The card can be registered using Paybox System (redirect) or Paybox Direct, the registration method used does not change the request method for the debit. In the request the previously obtained token must be placed as the card number, the expiry date also needs to be provided.

**Request:**

```
VERSION=00104&TYPE=00053&SITE=1999888&RANG=32&CLE=1999888I&NUM  
QUESTION=194102423&MONTANT=1000&DEWISE=978&REFERENCE=TestPaybo  
x&PORTEUR=SLDLrcsLMPC&DATEVAL=0520&REFABONNE=ABODOCUMENTATION0  
01&ACTIVITE=027&DATEQ=30012013&PAYS=
```

**Response:**

```
NUMTRANS=0001480206&NUMAPPEL=0002269499&NUMQUESTION=0194102423  
&SITE=1999888&RANG=32&AUTORISATION=XXXXXX&CODEREponse=00000&CO  
MMENTAIRE=Demande traitée avec  
succès&REFABONNE=ABODOCUMENTATION001&PORTEUR=SLDLrcsLMPC&PAYS=  
???
```



- Authorization Response:

Jan 29 09:07:15 pbxprwb56 PPS.php[21673]: [INFO] Retour ruffdponse :  
SITE=xxxxxxx&RANG=0XX&NUMQUESTION=0000000089&IDENTIFIANT=xxxxxxx&CO  
MMENTAIRE=OK&NUMAPPEL=0179527924&NUMTRANS=0170435393&AUTORISATION  
=352757&PAYS=BEL&SHA-  
1=C04A6609625600AF0AF025058B23B3238ABF3DCD&CODEREPOSE=00000

## 9.6 GLOSSARY

### 9.6.1 3-D Secure

The 3-D Secure protocol has been defined by VISA and MASTERCARD in order to solve 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.

Verifone 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 or by his bank which can require this activation in case of too many charge-backs.

Verifone 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 under the mention **Statut Porteur 3D Secure**.

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

- 1 – Verifone checks online with Visa and MasterCard if the card is enrolled in the 3-D Secure program
- 2 – Verifone 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 of responsibility (or Guarantee) are based on those messages and phases.

For every payment, Verifone can provide the result of those messages and phases.

For more information, please consult our information sheet: **[Ref 4] « Fiche presentation 3-D Secure »**.

### 9.6.1 URL Encoding

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.

### 9.6.2 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.

### 9.6.3 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.

### 9.6.4 HTTP

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

### 9.6.5 IP (adresse IP)

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

### 9.6.6 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.

### 9.6.7 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>