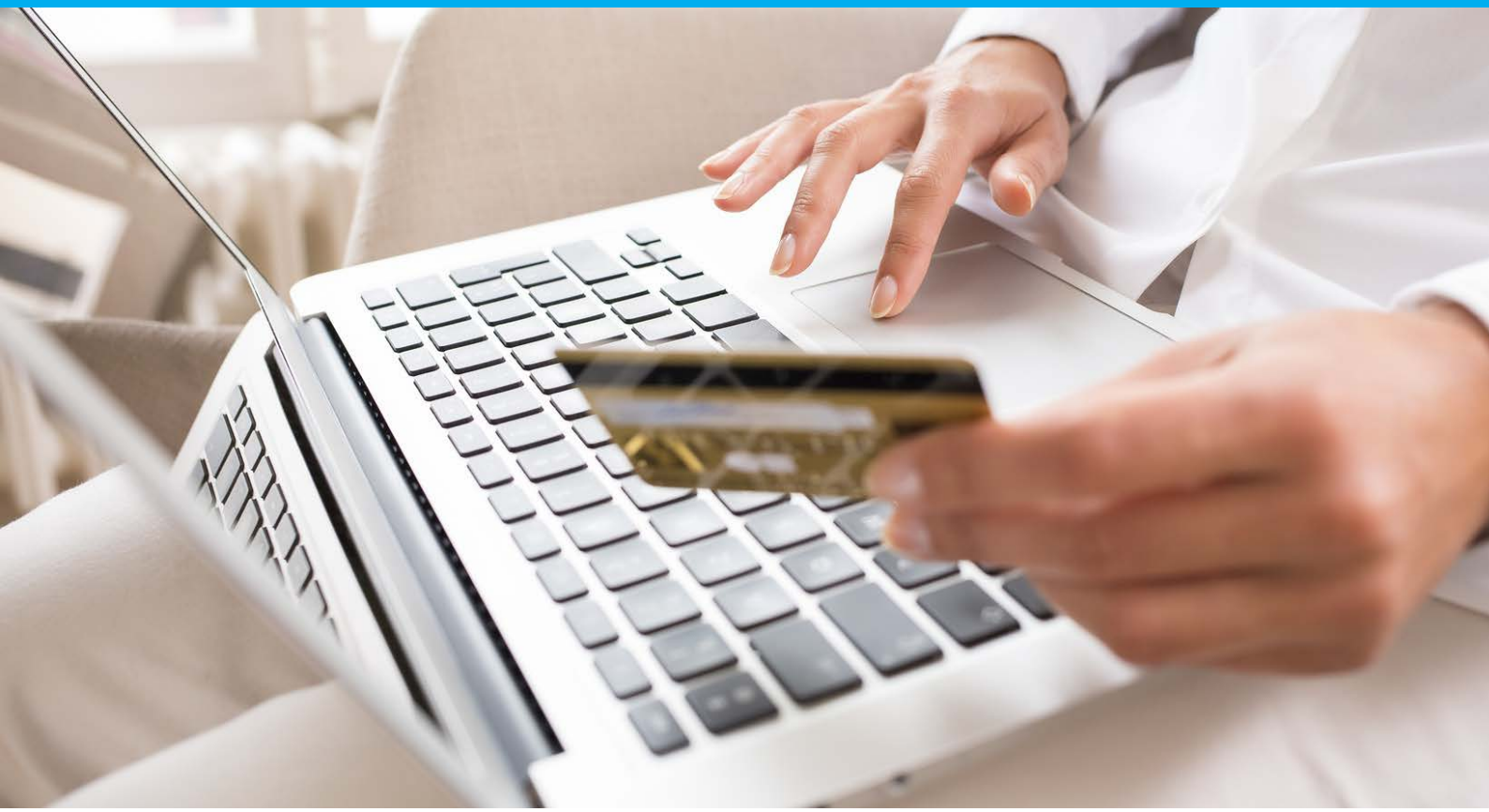


# Remote MPI
# 3-D Secure / Safekey

## Integration Manual

## Version 8.0

---

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

# CHANGE REVIEW

| DATE | VERSION | DESCRIPTION | AUTEUR |
|---|---|---|---|
| 2016-10-23 | 7.00 | Presentation of a second integration | M. THOMAS |
| 2016-11-28 | 7.1 | Remote MPI Update (American Express Safekeyintegration) | Anthony Henique |
| 2017-07-03 | 8.0 | Update corporate identity and style guide | Project 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 | ManuelIntegrationVerifone_PayboxDirect_V8.1_EN.docx | Integration guide for Paybox Direct |
| Ref 2 | ParamètresTestVerifone_Paybox_V8.0_EN.docx | Manual explaining the test environment and the test accounts (pre-production). |
| Ref 3 | ManuelIntegrationVerifone_PayboxSystem_V8.0_EN.docx | Integration guide for Paybox System |
| Ref 4 | GUIDE_UTILISATEUR_BACK_OFFICE_COMMERCANT_PAYBOX.doc | Product information on 3-D Secure / American Express Safekey and advantages for the merchant. |
| Ref 5 | PAYBOX Fiche présentation 3DSecure.pdf | 3-D Secure presentation note. |

# 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



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

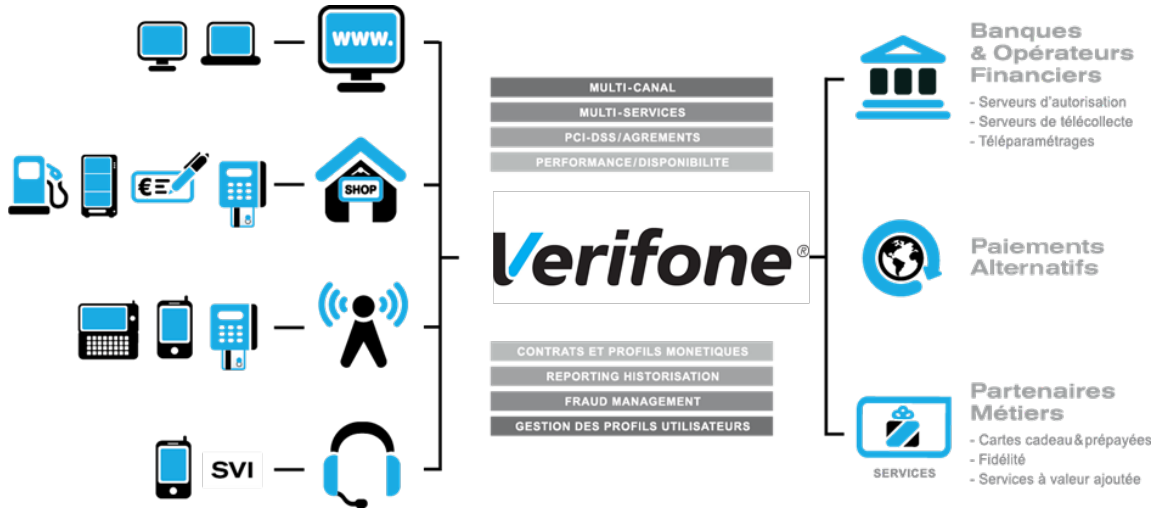

For any contact with our Sales service or Technical and client Helpdesk, you must provide the following Verifone identifiers:

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

# SUMMARY

# 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 Verifone 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 Verifone 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.

The goal of this document is to describe how to add the 3-D Secure / American Express Safekey authentication to the PAYBOX DIRECT service.

When using 3-D Secure / American Express Safekey an extra step for cardholder authentication is executed before an authorization request is submitted and where it is appropriate the results of the authentication are added to the authorization request.

# 3. « PAYBOX REMOTE MPI » PRESENTATION

## 3.1 MPI AND 3-D SECURE / AMERICAN EXPRESS SAFEKEY

The MPI (**M**erchant **P**lug-**I**n) is a software module that is installed on the Verifone servers. The module allows for authentication of 3 participants in the transactions (Merchant, Cardholder and Issuer bank) through an interoperable exchange of messages according to the 3-D Secure / American Express Safekey standard.

This same module is integrated in PAYBOX System and provides the 3-D Secure / American Express Safekey service through the browser of the customer.

The exchange of messages adheres to the standard defined by Visa / Mastercard and American Express and uses 2 pairs of messages:

1) The first pair of messages will verify on the Directory Server of Visa / Mastercard or American Express that the card entered by the cardholder can participate in the 3-D Secure / American Express Safekey program (it is said “cardholder is enrolled”).

   The two messages of the first pair are the **VEReq** (Verify Enrollment Request) and the **VERes (**Verify Enrollment Response).

2) In the case that it is confirmed that the card is enrolled for the 3-D Secure / American Express Safekey programme, a second pair of message is exchanged by redirecting the cardholder to the bank tha issued him the card ('issuer' bank) for authentication.

   The two messages of the second message pair are the **PAReq** (Payer Authentication Request) and the **PARes** (Payer Authentication Response).

The result of these exchanges will either allow or prevent to continue with an authorisation request towards the PAYBOX DIRECT service.

The architecture of the PAYBOX 'Remote MPI' has been designed to meet 2 criteria:

**Compliance with the Visa / Mastercard and American Express regulations**

The data elements returned are those returned by the MPI and according to the format as specified in the Visa / Mastercard and American Express standard...

**Easy integration with the existing PAYBOX DIRECT interfaces**

The necessary 3-D Secure / American Express Safekey data element required for the authorisation request are stored in a PAYBOX context.

A unique identifier towards this context is returned at the end of the 3-D Secure / American Express Safekey authentication session and can then be reinjected into the PAYBOX DIRECT interface. This identifier allows to recuperate the corresponding 3-D Secure / American Express Safekey data elements for the current authorisation request.

This context identifier only points to the 3-D Secure / American Express Safekey authentication data elements. It is required to fill in all the other mandatory data elements necessary for the PAYBOX DIRECT interface to work. (see ***Ref 1 ManuelIntegrationVerifone_PayboxDirect_V8.1_EN.docx***).

**OR**

**Possibility to use Paybox Direct without context**

The context shown below can't be used when you integrate the product Paybox Direct. In this case, it will be necessary to provide all the information returned by the product RemoteMPI after a 3-D Secure / American Express Safekey authentication (see ***Ref 1 ManuelIntegrationVerifone_PayboxDirect_V8.1_EN.docx***)

## 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<br>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<br>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 at Verifone 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

A CGI script installed on the PAYBOX SERVICES infrastructure gives access to the PAYBOX MPI. This CGI can be called through the follow URL:

- https://tpeweb.paybox.com/cgi/RemoteMPI.cgi

or

- https://tpeweb1.paybox.com/cgi/RemoteMPI.cgi

or

- https://tpeweb2.paybox.com/cgi/RemoteMPI.cgi

or

- https://tpeweb0.paybox.com/cgi/RemoteMPI.cgi

In case one URL is not responding, you can call the other URL.

To start the cardholder authentication, you need to redirect the client to one of these URL and send the parameters as described later with the POST method.

The list of parameters you have to send is described in the chapter **§8 Data Dictionary**

Exemple d'appel via un formulaire HTML :

```
<html>
<body>

<form action="https://preprod-tpeweb.paybox.com/cgi/RemoteMPI.cgi" method="post">

<input name="IdMerchant" value="109518543" type="hidden">
<input name="IdSession" value="DOC001" type="hidden">
<input name="Amount" value="1000" type="hidden">
<input name="Currency" value="978" type="hidden">
<input name="CCNumber" value="1111222233334444" type="hidden">
<input name="CCExpDate" value="1014" type="hidden">
<input name="CVVCode" value="123" type="hidden">
<input name="URLRetour" value="https://maboutique.com/retour.php" type="hidden">
```

## 4.2 RESPONSE

There are two groups of parameters that are returned.

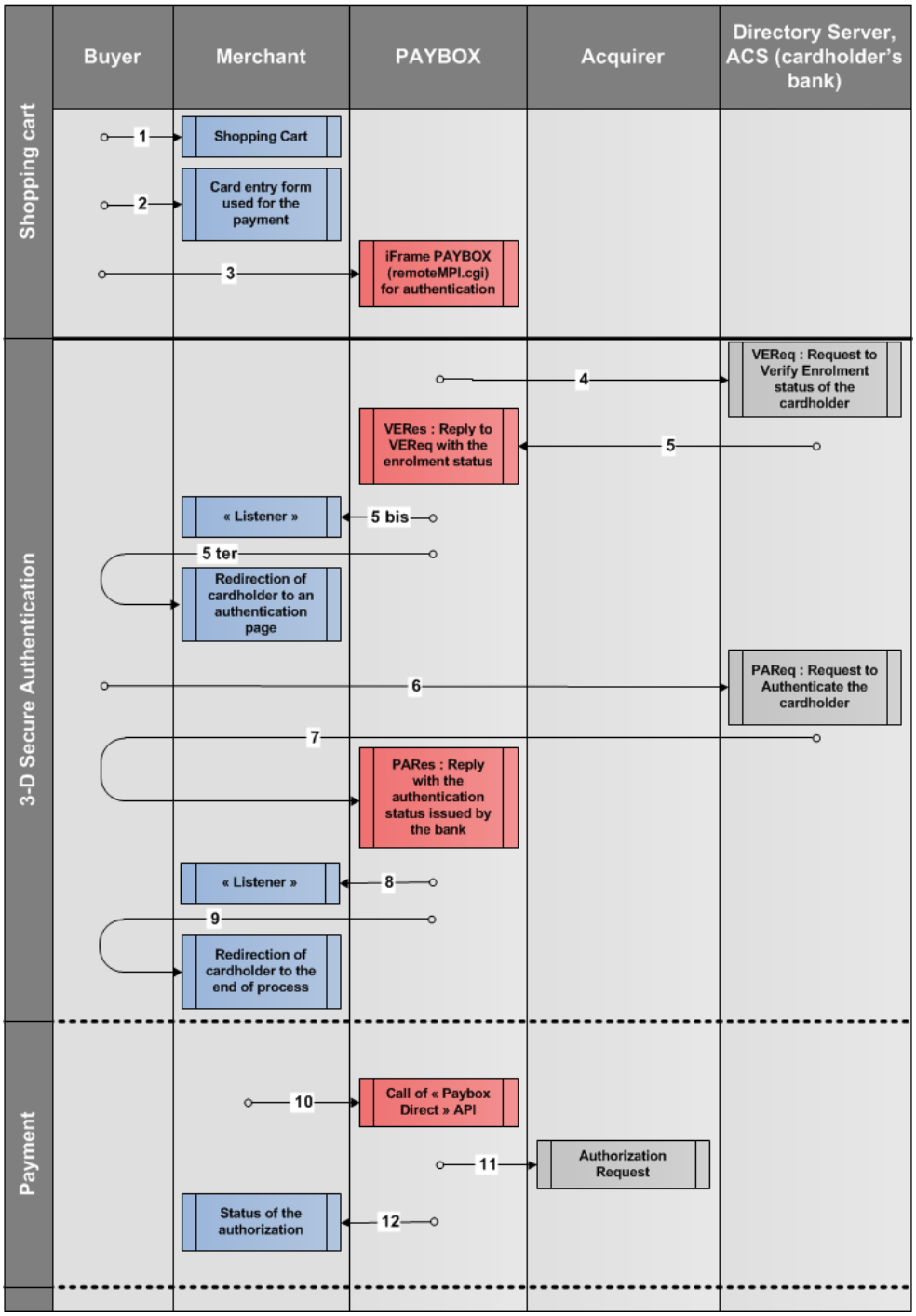
- The parameters used for the technical integration
  - ID3D
  - StatusPBX
  - Check
- The specific 3-D Secure / American Express Safekey parameters as a result of the MPI, they are either for information (if you use the ID3D context with the product Paybox Direct) or to be used when calling the product Paybox Direct without the ID3D context.

If the variable StatusPBX has the value « **Autorisation à faire** », you can send an authorization request with Paybox Direct.

To refer to this authentication context, you also need to get the content of the ID3D variable sent by RemoteMPI and transmit it in the Paybox Direct request.

- The Paybox Direct request must be issued immediatly after the MPI response. After a delay of 5 minutes, the authentication is considered expired and Paybox will not emit an authorization request to the acquirer.
- In case of invalid parameters sent to the program, only the IdSesion, StatusPBX and Check fields are returned when the parameters check are OK.

# 5. FLOW OF A PAYMENT WITH 3-D SECURE/SAFEKEY USING PAYBOX DIRECT



| STEP | IMPACT MERCHANT | DESCRIPTION |
|---|---|---|
| 1 | Yes | The shopper is making an order on the website of the merchant. |
| 2 | Yes | The buyer is entering his card details (PAN, expiry date, visual cryptogram) on the website of the merchant. |
| 3 | Yes | The merchant is redirecting the cardholer to a PAYBOX URL for 3-D Secure / American Express Safekey authentication. |
| 4 | No | The directory server of the scheme (Visa / Mastercard or American Express) is contacted in order to verify the enrollment of the card/cardholder. |
| 5 | No | The enrollment status and the URL of the issuer authentication infrastructure (if applicable) is return. |
| 5 bis | Yes | This step is only executed in one of the following 3 cases:<br>1) Error while accessing the MPI<br>2) Error during transmission of the VEReq/VERes<br>in the case 1) and 2) :<br>**The ID3D context identifier is not returned.**<br>**However an authorisation request can be submitted to the PAYBOX Direct interface, but without the ID3D parameter or without the 3-D Secure / American Express Safekey variables if you don't use the ID3D context variable.**<br>3) The cardholder is not enrolled<br>**The ID3D context identifier is returned.**<br>**A non 3-D Secure / American Express Safekey authorisation request can be submitted to the PAYBOX Direct interface with the ID3D parameter or with the 3-D Secure / American Express Safekey variables if you don't use the ID3D context variable.**<br>The steps 6 to 9 are then not executed in this scenario.<br>The cardholder is simply redirected to a webpage on the merchant website. |
| 5 ter | Yes | In case the card/cardholer is not enrolled in the 3-D Secure / American Express Safekey program, the cardholder is redirected to a webpage on the merhant's website. |
| 6 | No | This step only happens in case of not enrolled and steps 6 to 9 are skipped. |
| 7 | No | The cardholer is redirected to his issuer for authentication. |
| 8 | Yes | The outcome of the authentication of the cardholder is returned. |

| | | |
|---|---|---|
| 9 | Yes | Confirmation (server to server) of the outcome of the authentication of the cardholder and wether or not to proceed with the payment. |
| 10 | Yes | Call of the « Paybox Direct » API to initiate the authorization request to the acquirer.<br><br>Cardholder's authentication data is stored for 5 minutes on Paybox by the identifier ID3D. This identifier must be added to the other variables sent to the Paybox Direct API.<br><br>If you choose to integrate the product Paybox Direct without using the ID3D context variable, other variables 3-D Secure / American Express Safekey should be present when calling to Paybox Direct API. |
| 11 | No | Authorization request sent from Paybox to the acquirer bank |
| 12 | Yes | Authorization response sent in reply to the message sent on step 10 |

# 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

+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 Verifone web site ***www.paybox.com***, or send an email to **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] « **ParamètresTestVerifone_Paybox_V8.0_EN.pdf**» available for download here:

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

# 8. DATA DICTIONARY

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

| VARIABLE | REQUEST | RESPONSE | DESCRIPTION |
|---|---|---|---|
| Amount | X | | Amount of the authorization request |
| CCExpDate | X | | Card expiry date |
| CCNumber | X | | Card number |
| Currency | X | | Currency used for the transaction |
| CVVCode | X | | Visual cryptogram of the card |
| IdMerchant | X | | Merchant id provided by Verifone |
| IdSession | X | X | Unique session id |
| URLHttpDirect | X | | Return URL - server-to-server |
| URLRetour | X | | Return URL – client browser |
| 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 3-D 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 |
| Check | | X | Paybox Signature |
| ID3D | | X | Paybox context id |
| StatusPBX | | X | Authentication request status |

**Table 1: Overview of all Paybox Remote MPI parameters**

# 8.1 PARAMETERS USED IN A REMOTE MPI CALL

## 8.1.1 Amount

Format: Numerical. **Mandatory.**

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

- Same amount must be used for Remote MPI authentication request and Paybox Direct authorization request.

Example: for 19€90 - 0000001990

Equivalent Paybox Direct : MONTANT

## 8.1.2 CCExpDate

Format: Date (MMYY) **Mandatory.**

Expiry date of the card.

Example: 1218 (december 2018)
Equivalent Paybox Direct : DATEVAL

## 8.1.3 CCNumber

Format: up to 19 characters. **Mandatory.**

PAN (card number) of the customer.

Example: 1111222233334444
Equivalent Paybox Direct : PORTEUR

## 8.1.4 Currency

Format: 3 digit. **Mandatory.**

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.

Equivalent Paybox Direct: DEVISE

## 8.1.5 CVVCode

Format: 3 or 4 characters. **Mandatory for requests of type 1, 3, 4, 12.**

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
Equivalent Paybox Direct : CVV

### 8.1.6 IdMerchant

Format: Numerical. **Mandatory.**

Merchant id provided by Verifone during subscription.

Example: 2

### 8.1.7 IdSession

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

Unique request id designed to prevent confusion between responses when sending several questions at the same time.
Each call must have a unique question number for a merchant.

Example: Session001

### 8.1.8 URLHttpDirect

Format: up to 250 characters.

Server to server callback URL. If this field is not sent, Verifone will use the one requested during merchant subscription.

Example: http://maboutique.com/retourMPI.php

### 8.1.9 URLRetour

Format: up to 250 characters.

Client brower callback URL. If this field is not sent, Verifone will use the one requested during merchant subscription.

## 8.2 RETURN PARAMETERS PAYBOX REMOTE MPI

### 8.2.1 IdSession

Format: up to 250 characters.

Unique request id designed to prevent confusion between responses when sending several questions at the same time.
Each call must have a unique question number for a merchant.

Example: Session001

### 8.2.2 StatusPBX

Format : Alphanumerical.

Authentication request status (possible values listed below).
Conditioned the authorization call send to PAYBOX Direct.

| STATUSPBX | DESCRIPTION |
|---|---|
| **Erreur Paybox** | Sent when Paybox application encountered an error.<br>Cardholder authentication failed and authorization request must not me sent. Authentication should be attempted again. |
| Autorisation à faire | Sent after authentication attempt, payment can be done after an authorization attempt. |
| Autorisation à ne pas faire | Sent after authentication attempt, authorization attempt must not be attempted. Cardholder authentication failed. |
| Timeout | Sent after 5 minutes timeout if the cardholder did not respond. |

### 8.2.3 ID3D

Format: up to 20 digits

Verifone context id containing authentication data provided by the MPI.
This authentication context is store for 5 minutes.
After 5 minutes context will timeout and Paybox will act as if cardholder authentication was invalid.

Example: 9900000000012

### 8.2.4 Check

Format: up to 256 characters.

Electronic signature from Paybox, calculated on all data provided.

See: ***Ref 3 ManuelIntegrationVerifone_PayboxSystem_V8.0_EN.docx*** for more detail on signature calculation. During RemoteMPI implementation, data must be URL encoded for signature validation.

### 8.2.5 3DCAVV

Format: 28 characters.

Value received from ACS. Encoding Base64.
This variable must be transmited through Paybox Direct if context ID3D is not used.
This variable must not be URL encoded when sent to Paybox Direct.

Example: jNEEdZ7c5MThARFVdvTZKmZSAUc=

### 8.2.6 3DCAVVALGO

Format: up to 64 characters

Id of the algorithm used for cardholder authentication by the ACS.
This variable must be transmited through Paybox Direct if context ID3D is not used.

Example: 0000000001

### 8.2.7 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.

### 8.2.8 3DENROLLED

Format: 1 character

Status of the 3D 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

### 8.2.9 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.

See also: ***§9.1.2 MPI error codes***

### 8.2.10 3DSIGNVAL

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

### 8.2.11 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

### 8.2.12 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: IC8wlK1CVDB2b4w9Hme63bmz/w4=

# 9. ANNEXES

## 9.1 RESPONSE CODE

### 9.1.1 Error code from Remote MPI

Program checks all of the parameters send and sent an error code when needed (see table below).

This message is not related to an error from the MPI.

There is no validation of URLs (URLRetour and URLHttpDirect)

| CODE | SIGNIFICATION |
|---|---|
| 1 | Error access configuration file (intern Paybox) |
| 2 | Error access to connections parameters for databases |
| 3 | Error accessing local context variables. |
| 4 | Error accessing pathfile to the MPI (MPI_PATH) |
| 5 | Error database connection. |
| 6 | Error preparation to search for site (fsite) |
| 7 | Error preparation to search for transactions MPI (TransMPI) |
| 101 | Error missing amount (Amount) |
| 102 | Error missing expiration date (CCExpdate) |
| 103 | Error missing cardholder number (CCNumber) |
| 104 | Error missing devise (Currency) |
| 105 | Error missing id merchant (IdMerchant) |
| 106 | Error missing merchant sessions id (IdSession) |
| 107 | Error missing merchant reference. (RefMarchant) |
| 108 | Error missing transMPI id |
| 110 | Error cardholder number size |
| 111 | Error cardholder number type |
| 112 | Error amount type |

| | |
|---|---|
| 113 | Error merchant reference size |
| 114 | Error expiration date size |
| 115 | Error expiration date type |
| 116 | Error expiration date value |
| 117 | Error CVV length (optional) |
| 118 | Error TransMPI id lenght |
| 201 | Error searching for site |
| 202 | Error searching for TransMPI |
| 301 | Error adding TransMPI record |
| 401 | Error merchant reference size |
| 402 | Size error on MPI error code |
| 403 | XID siez error |
| 410 | Error merchant reference missing |
| 411 | Error merchant reference type |
| 412 | Error on error code type |

**Table 2 : Remote MPI response code**

### 9.1.2 MPI error codes

These codes can be sent in variable 3DERROR

| CODE | SIGNIFICATION |
|---|---|
| 0 | No Error |
| 100 | AuthReq received is invalid |
| 101 | Merchant is not known |
| 102 | Merchant is not active |
| 103 | invalid referrer |
| 104 | An error occured during processing |

| | |
|---|---|
| 105 | Currency is not supported |
| 106 | Transaction not found |
| 107 | Brand is not supported |
| 108 | The validation post to the merchant failed |
| 1300 | the HTTP return code is not found |
| 1301 | the HTTP return code is not valid |
| 1302 | the received message contains no XML |
| 1303 | not possible to import the xml in JDOM |
| 1304 | incorrect root element |
| 1305 | the element message is not defined |
| 1306 | the attibuut id is not defined for |
| 1307 | the attibuut id is not defined for Extension |
| 1308 | the attibuut id and critical are not defined for Extension |
| 1309 | the attibuut critical is not defined for Extension |
| 1310 | the element Extension is not correct |
| 1311 | the element version is not found |
| 1312 | the version of the ThreeDSecureMessage is too old |
| 1313 | the attribute critical is defined for Extension with value true |
| 1314 | Root element invalid |
| 1315 | Message element not found or invalid |
| 1330 | CRReq - the element Merchant is not found |
| 1331 | CRReq - the element acqBIN is not found |
| 1332 | CRReq - the element merID is not found |
| 1333 | CRReq - the element password is not found |
| 1334 | CRReq - the element CRReq is not found |
| 1335 | CRReq - the element version is not valid |

| | |
|---|---|
| 1336 | CRReq - the element Merchant.acqBIN is not valid |
| 1337 | CRReq - the element Merchant.merID is not valid |
| 1338 | CRReq - the element Merchant.password is not valid |
| 1339 | CRReq - the element serialNumber is not valid |
| 1350 | CRRes - the element begin is not found |
| 1351 | CRRes - the element end is not found |
| 1352 | CRRes - the element action is not found |
| 1353 | CRRes - the element CRRes is not found |
| 1354 | CRRes - the element serialnumber is not found |
| 1355 | CRRes - the element version is not valid |
| 1356 | CRRes - the element begin is not valid |
| 1357 | CRRes - the element end is not valid |
| 1358 | CRRes - the element action is not valid |
| 1359 | CRRes - the element serialNumber is not valid |
| 1360 | CRRes - the element vendorcode is too long |
| 1361 | CRRes - the element iReqCode is not found |
| 1362 | CRRes - the element IReqCode has bad format |
| 1401 | VEReq - the element pan is not found |
| 1402 | VEReq - the element Merchant is not found |
| 1403 | VEReq - the element acqBIN is not found |
| 1404 | VEReq - the element merID is not found |
| 1405 | VEReq - the element password is not found |
| 1406 | VEReq - the element VEReq is not found |
| 1407 | VEReq - the element version is not valid |
| 1408 | VEReq - the element pan is not valid |
| 1409 | VEReq - the element Merchant.acqBIN is not valid |

| | |
|---|---|
| 1410 | VEReq - the element Merchant.merID is not valid |
| 1411 | VEReq - the element Merchant.password is not valid |
| 1412 | VEReq - the element Merchant.password is not valid |
| 1501 | VERes - the element VERes is not found |
| 1502 | VERes - the element version is not valid |
| 1503 | VERes - the element enrolled is not valid |
| 1504 | VERes - the element accId is empty |
| 1505 | VERes - the element accId is to long |
| 1506 | VERes - the element url is empty |
| 1507 | VERes - the element url has a bad protocol |
| 1508 | VERes - the element url is malformed |
| 1509 | VERes - the element protocol is empty |
| 1510 | VERes - the element protocol is not valid |
| 1511 | VERes - the element vendorcode is too long |
| 1512 | VERes - the element CH is not found |
| 1513 | VERes - the element enrolled is not found |
| 1514 | VERes - the element acctid is not found |
| 1515 | VERes - the element url is not found |
| 1516 | VERes - the element protocol is not found |
| 1517 | VERes - the element IReq is not found |
| 1518 | VERes - the element iReqCode is not found |
| 1519 | VERes - the element IReqCode has bad format |
| 1520 | VERes - the element acctId is the same as the pan |
| 1601 | PAReq - the element version is not valid |
| 1602 | PAReq - the element PAReq is not found |
| 1603 | PAReq - the element Merchant is not found |

| | |
|---|---|
| 1604 | PAReq - the element acqBIN is not found |
| 1605 | PAReq - the element merID is not found |
| 1606 | PAReq - the element name is not found |
| 1607 | PAReq - the element country is not found |
| 1608 | PAReq - the element url is not found |
| 1609 | PAReq - the element Purchase is not found |
| 1610 | PAReq - the element xid is not found |
| 1611 | PAReq - the element date is not found |
| 1612 | PAReq - the element amount is not found |
| 1613 | PAReq - the element purchAmount is not found |
| 1614 | PAReq - the element currency is not found |
| 1615 | PAReq - the element exponent is not found |
| 1616 | PAReq - the element frequency is not found |
| 1617 | PAReq - the element endRecur is not found |
| 1618 | PAReq - the element CH is not found |
| 1619 | PAReq - the element CH.acctID is not found |
| 1620 | PAReq - the element CH.expiry is not found |
| 1621 | PAReq - the element Merchant.acqBIN is not valid |
| 1622 | PAReq - the element Merchant.merID is not valid |
| 1623 | PAReq - the element Merchant.name is not valid |
| 1624 | PAReq - the element Merchant.country is not valid |
| 1625 | PAReq - the element Merchant.url is not valid |
| 1626 | PAReq - the element url is empty |
| 1627 | PAReq - the element url has a bad protocol |
| 1628 | PAReq - the element url is malformed |
| 1629 | PAReq - the element xid has bad format |

| | |
|---|---|
| 1630 | PAReq - the element date has bad format |
| 1631 | PAReq - the element amount has bad format |
| 1632 | PAReq - the element purchAmount has bad format |
| 1633 | PAReq - the element currency has bad format |
| 1634 | PAReq - the element exponent has bad format |
| 1635 | PAReq - the element desc has bad format |
| 1636 | PAReq - the element frequency has bad format |
| 1637 | PAReq - the element endRecur has bad format |
| 1638 | PAReq - the element install has bad format |
| 1639 | PAReq - the element acctID has bad format |
| 1640 | PAReq - the element expiry has bad format |
| 1641 | PAReq - the element exponent is not numeric |
| 1642 | PAReq - the element gmtOffset is not found |
| 1643 | PAReq - the element brands is not found |
| 1644 | PAReq - the element desc is not found |
| 1645 | PAReq - the element pan is not found |
| 1646 | PAReq - the element gmtOffset is not valid |
| 1647 | PAReq - the element brands is not valid |
| 1648 | PAReq - the element recurring is not valid |
| 1649 | PAReq - the element installment is not valid |
| 1701 | PARes - the element PARes is not found |
| 1702 | PARes - the element version is not valid |
| 1703 | PARes - the element Merchant.acqBIN is not valid |
| 1704 | PARes - the element Merchant.merID is not valid |
| 1705 | PARes - the element xid has bad format |
| 1706 | PARes - the element date has bad format |

| | |
|---|---|
| 1707 | PARes - the element amount has bad format |
| 1708 | PARes - the element purchAmount has bad format |
| 1709 | PARes - the element currency has bad format |
| 1710 | PARes - the element exponent has bad format |
| 1711 | PARes - the element exponent is not numeric |
| 1712 | PARes - the element TX.time is not valid |
| 1713 | PARes - the element TX.status is not valid |
| 1714 | PARes - the element pan is not valid |
| 1715 | PARes - the element TX.cavv is not valid |
| 1716 | PARes - the element TX.eci is not valid |
| 1717 | PARes - the element TX.cavvAlgorithm is not valid |
| 1718 | PARes - the element IReq.iReqCode is not valid |
| 1719 | PARes - the element IReq.vendorCode is not valid |
| 1720 | PARes - the element desc is not valid |
| 1721 | PARes - the element CH.exp is not valid |
| 1722 | PARes - the element TX.detail is not valid |
| 1723 | PARes - the element TX.stain is not valid |
| 1724 | PARes - the element TX.vendorCode is not valid |
| 1725 | PARes - the element TX.eci is not valid |
| 1726 | PARes - the element Merchant is not found |
| 1727 | PARes - the element acqBIN is not found |
| 1728 | PARes - the element merID is not found |
| 1729 | PARes - the element Purchase is not found |
| 1730 | PARes - the element xid is not found |
| 1731 | PARes - the element date is not found |
| 1732 | PARes - the element purchAmount is not found |

| | |
|---|---|
| 1733 | PARes - the element currency is not found |
| 1734 | PARes - the element exponent is not found |
| 1735 | PARes - the element pan is not found |
| 1736 | PARes - the element tx is not found |
| 1737 | PARes - the element time is not found |
| 1738 | PARes - the element status is not found |
| 1739 | PARes - the element cavv is not found |
| 1740 | PARes - the element eci is not found |
| 1741 | PARes - the element cavvAlgorithm is not found |
| 1742 | PARes - the element iReqCode is not found |
| 1743 | PARes - the element Purchase.currency has not the same value as the one in the PAReq |
| 1744 | PARes - the element Purchase.exponent has not the same value as the one in the PAReq |
| 1745 | the Signature.xmlns namespace is not found |
| 1746 | the Signature.xmlns namespace has a bad format |
| 1747 | the Signature.SignedInfo has a bad format |
| 1748 | the Signature.CanonicalizationMethod has a bad format |
| 1749 | the Signature.CanonicalizationMethod has different namespace |
| 1750 | the Signature.SignatureMethod has a bad format |
| 1751 | Signature.SignatureMethod has different namespace |
| 1752 | Signature.SignedInfo.Reference.URI not found |
| 1753 | Signature.SignedInfo.Reference.URI has a bad format |
| 1754 | Signature.SignedInfo.Reference.DigestValue not found |
| 1755 | Signature.SignatureValue not found |
| 1756 | Signature.KeyInfo not found |
| 1801 | Error - the element Error is not found |

| | |
|---|---|
| 1802 | Error - the element version is not valid |
| 1803 | Error - the element errorCode is not valid |
| 1804 | Error - the element errorMessage is empty |
| 1805 | Error - the element errorDetail is empty |
| 1806 | Error - the element vendorCode is too long |
| 1807 | Error - the element errorCode is not found |
| 1808 | Error - the element errorMessage is not found |
| 1809 | Error - the element errorDetail is not found |
| 1901 | PATransReq - the element PATransReq is not found |
| 1902 | PATransReq - the element version is not valid |
| 1903 | PATransReq - the element Merchant.name is not valid |
| 1904 | PATransReq - the element Merchant.country is not valid |
| 1905 | PATransReq - the element Merchant.url is not valid |
| 1906 | PATransReq - the element amount is not found |
| 1907 | PATransReq - the element url is empty |
| 1908 | PATransReq - the element url has a bad protocol |
| 1909 | PATransReq - the element url is malformed |
| 1910 | PATransReq - the element amount has bad format |
| 1911 | PATransReq - the element desc has bad format |
| 1912 | PATransReq - the element frequency has bad format |
| 1913 | PATransReq - the element endRecur has bad format |
| 1914 | PATransReq - the element install has bad format |
| 1915 | PATransReq - the element date has bad format |
| 1916 | PATransReq - the element name has bad format |
| 1917 | PATransReq - the element fullpan has bad format |
| 1918 | PATransReq - the element expiry has bad format |

| | |
|---|---|
| 1919 | PATransReq - the element acs Id id has bad format |
| 1920 | PATransReq - the element login Id has bad format |
| 1921 | PATransReq - the element password has bad format |
| 1922 | PATransReq - the element signed pares has bad format |
| 1925 | PATrans - the element version is not valid |
| 1926 | PATrans - the element PATransReq is not found |
| 1927 | PATrans - the element Merchant.id is not found |
| 1928 | PATrans - the element Merchant.name is not valid |
| 1929 | PATrans - the element Merchant.country is not valid |
| 1930 | PATrans - the element Merchant.url is not valid |
| 1931 | PATrans - the element Purchase.id is not found |
| 1932 | PATrans - the element Purchase.xid is not found |
| 1933 | PATrans - the element Purchase.date is not valid |
| 1934 | PATrans - the element Purchase.amount is not valid |
| 1935 | PATrans - the element Purchase.rawamount is not valid |
| 1936 | PATrans - the element Purchase.currency is not valid |
| 1937 | PATrans - the element Purchase.desc is not valid |
| 1938 | PATrans - the element Purchase.recurring is not valid |
| 1939 | PATrans - the element Purchase.installment is not valid |
| 1940 | PATrans - the element CH.name is not valid |
| 1941 | PATrans - the element CH.pan is not valid |
| 1942 | PATrans - the element CH.exp is not valid |
| 1943 | PATrans - the element TX.time is not valid |
| 1944 | PATrans - the element TX.status is not valid |
| 1945 | PATrans - the element TX.detail is not valid |
| 1946 | PATrans - the element TX.stain is not valid |

| | |
|---|---|
| 1947 | PATrans - the element TX.eci is not valid |
| 1948 | PATrans - the element TX.vendorCode is not valid |
| 1949 | PATrans - the element SignedPARes is not valid |
| 1951 | PATransRes - the element PATransRes is not found |
| 1952 | PATransRes - the element version is not valid |
| 1953 | PATransRes - the element iReq.IReqCode is not found |
| 1954 | PATransRes - the element iReq.IReqCode is not found |
| 1955 | PATransRes - the element iReq.IReqCode is not valid |
| 1956 | PATransRes - the element iReq.IReqCode is not valid |
| 1971 | CAVV - the element xid is not found |
| 1972 | CAVV - the element pan is not valid |
| 1973 | CAVV - the element authResultCode is not valid |
| 1974 | CAVV - the element secondFactorAuthCode is not valid |
| 1975 | CAVV - the element cavvKeyIndicator is not valid |
| 1976 | CAVV - the element cardSequenceNumber is not valid |
| 1977 | CAVV - the element cvr is not valid |
| 1978 | CAVV - the element unpredictableNumber is not valid |
| 1979 | CAVV - the element atn is not found |
| 5100 | Expiry date is invalid |
| 5101 | Pan not found in local cache |
| 5102 | No brand details foudn for that Merchant |
| 5103 | Error occured during validate of VEReq" |
| 5104 | Error occured during build of VEReq |
| 5105 | ThreeDSecureMessage Exception occured during validate and build of VEReq |
| 5106 | No connection details where found for that specific brand, merchant and pan |

| | |
|---|---|
| 5107 | Exception occured during the post of the VEReq message to the VisaDirectory |
| 5108 | Invalid Handler/ Locator or Generator configured during processing of VEReq |
| 5109 | Error occured during validate of Error" |
| 5110 | Error occured during build of Error |
| 5111 | ThreeDSecureMessage Exception occured during validate and build of Error |
| 5112 | Exception occured during the post of the Error message to the VisaDirectory |
| 5113 | Received an Error message instead of a VERes |
| 5114 | Unkown error |
| 5115 | Pan is not enrolled for 3-D Secure / American Express Safekey |
| 5116 | ThreeDSecure is not supported by the Issuer! |
| 5117 | Recieved a badly formatted VERes, so we had to send an error to the VSD |
| 5118 | Version is too old |
| 5119 | Currency code not found |
| 5120 | Error occured during validate of PAReq" |
| 5121 | ThreeDSecureMessage Exception occured during validate and build of PAReq |
| 5122 | No termUrl is found for the MPI |
| 5123 | Exception occured during creation of the PaReq Form |
| 5124 | Unknown error occured during processing of VERes |
| 5125 | Exception occured during decode and inflate of pares |
| 5126 | Recieved a badly formatted PARes, so we had to send an error to the VSD |
| 5127 | An error occured during the validation of the xml signature |
| 5128 | An error occured during the logging process of the PAReq message |

| | |
|---|---|
| 5129 | An error occured during the logging process of the PARes message |
| 5130 | An Exception occured when getting the PAReq from the cache, or during the parse and validate of it |
| 5131 | An Exception occured during encryption/decryption of sensative data |
| 5132 | An error occured during parse and validate of the VERes message |
| 5133 | An error occured during parse and validate of the PARes message |
| 5134 | The XML-signature of the PARes message is not a valid one |
| 5135 | Error occured during validate of CRReq |
| 5136 | Error occured during build of CRReq |
| 5137 | ThreeDSecureMessage Exception occured during validate and build of CRReq |
| 5138 | Exception occured during the post of the CRReq message to the VisaDirectory |
| 5139 | unknown error occure during processing of CRRes |
| 5140 | Recieved a badly formatted CRRes, so we had to send an error to the VSD |
| 5141 | Error occured during build of Veres |
| 5142 | Error occured during decode and inflate of PAReq |
| 5143 | Unable to start authentication flow |
| 5144 | Authentication was not successfull |
| 10000 | Unspecified error occured |
| 5145 | Error Getting VEReq out of transaction cache |
| 5146 | Received status U |
| 5147 | Received an Error message instead of a PARes |

**Tableau 3 : Codes réponses du MPI**

## 9.2 URL AND IP ADDRESSES TO CALL

In order to use **PAYBOX Remote MPI** :

| PLATE-FORME | URL TO CALL |
|---|---|
| **Preproduction** | https://preprod-tpeweb.paybox.com/cgi/RemoteMPI.cgi |
| **Principale** | https://tpeweb.paybox.com/cgi/RemoteMPI.cgi |
| **Secours** | https://tpeweb1.paybox.com/cgi/RemoteMPI.cgi<br>https://tpeweb2.paybox.com/cgi/RemoteMPI.cgi<br>https://tpeweb0.paybox.com/cgi/RemoteMPI.cgi |

**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 |
|---|---|---|
| **Preproduction** | 195.101.99.73 | 195.101.99.76 |
| **Production** | 194.2.160.66<br>194.2.160.80<br>194.2.160.82<br>194.2.160.91<br>195.25.7.146<br>195.25.67.0<br>195.25.67.2<br>195.25.67.11 | 194.2.122.158<br>194.2.122.190<br>195.25.7.166<br>195.25.67.22 |

# 9.3 GLOSSARY

## 9.3.1 3-D Secure / American Express Safekey

The 3-D Secure / American Express Safekey protocol has been defined by VISA and MASTERCARD in order to solve problem the problems of payment chargeback.

The 3-D Secure / American Express Safekey 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 / American Express Safekey 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 / American Express Safekey activation request can be issued by the merchant of 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 / American Express Safekey 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 / American Express Safekey payments with the parameter “Guarantee” in the Log menu.

More detailed information regarding the cardholder authentication is available under the mention Statut Porteur 3D

The 3-D Secure / American Express Safekey protocol is processed in 2 phases:

1 – Paybox checks online with Visa and MasterCard if the card is enrolled in the 3-D 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 and American Express concerning the transfer or 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 5] « Fiche présentation 3-D Secure ».***

### 9.3.2 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.

### 9.3.3 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.

### 9.3.4 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.

### 9.3.5 HTTP

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

### 9.3.6 IP (adress IP)

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

### 9.3.7 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.

### 9.3.8 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.

Exemple : `http://www.mystore.com/site/welcome.html`