



DSP2

Manuel d'intégration 3DSv2

Version 1.4

Verifone[®]

Verifone
12 rue Paul Dautier 78140 Vélizy-Villacoublay

HISTORIQUE DES MODIFICATIONS

DATE	VERSION	DESCRIPTION	AUTEUR
2020-04-01	1.0	Création.	Service Projet
2020-05-14	1.1	Ajout de Paybox Direct.	Service Projet
2020-07-02	1.2	Précisions pour Paybox Direct.	Service Projet
2020-09-15	1.3	Ajout des données de test.	Service Projet
2020-09-17	1.4	Ajustement de formulation et mise en page.	Service Projet

REFERENCES DOCUMENTATIONS

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

REF.	DOCUMENT	DESCRIPTION
Réf 1	ManuellIntegrationPayboxSystem_V8.0_FR.pdf	Manuel d'intégration de la solution Paybox System.
Réf 2	ManuellIntegrationPayboxDirect_V8.0_FR.pdf	Manuel d'intégration de la solution Paybox Direct / Direct +
Réf 3	ParametresTestPaybox_CB55_V8.0_FR.pdf	Paramètres de tests spécifiques à CB5.5.
Réf 4	ManuellIntegrationVerifone_RemoteMPI_V8.0_FR.pdf	Paybox Direct – Intégration 3-D Secure avec Remote MPI

LEGENDE

Les conventions suivantes s'appliquent dans la suite de ce document :

Une zone d'information : son contenu permet de mieux comprendre ce document.

Une zone d'avertissement : le contenu de cette zone doit être lu attentivement.

AVERTISSEMENT

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

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

INFORMATION & ASSISTANCE

Pour tout renseignement ou assistance à l'installation et à l'utilisation de nos produits, nos équipes restent à disposition des commerçants et intégrateurs :

Support Client et Technique

Lundi - vendredi 9h - 18h

support-paybox@verifone.com

0 825 305 004

Service 0,15 € / min
+ prix appel

Pour tout contact auprès de notre Support Client et Technique, il faut impérativement se munir de ses identifiants Paybox :

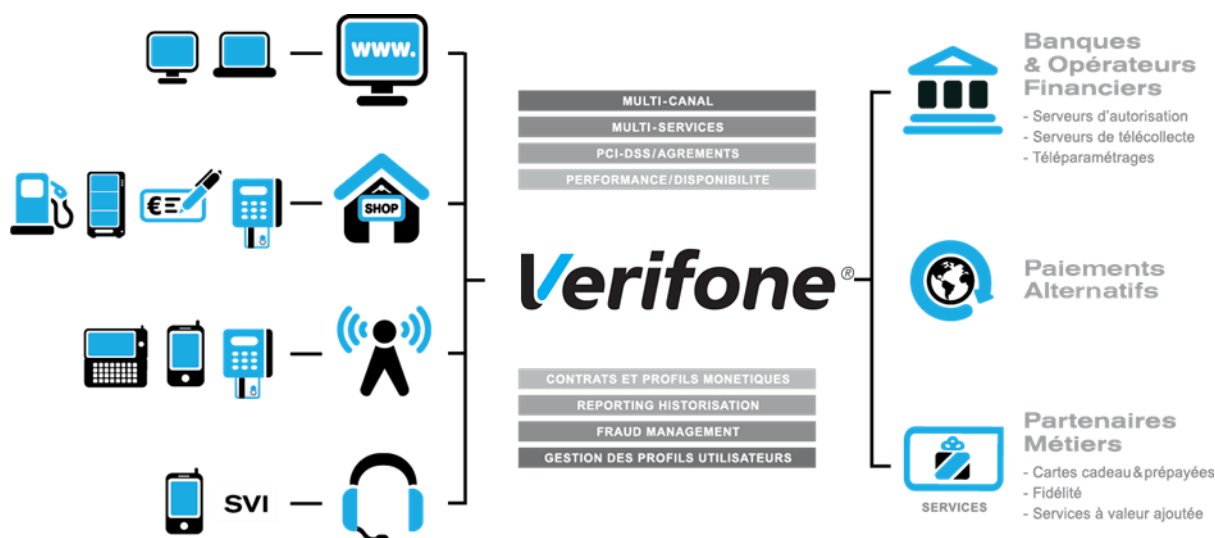
- Numéro de SITE (7 chiffres)
- Numéro de RANG (3 chiffres)
- Numéro d'identifiant Paybox (1 à 9 chiffres)

SOMMAIRE

HISTORIQUE DES MODIFICATIONS.....	2
REFERENCES DOCUMENTATIONS	3
LEGENDE	3
AVERTISSEMENT	4
INFORMATION & ASSISTANCE	4
SOMMAIRE.....	5
1. INTRODUCTION	6
2. OBJET DU DOCUMENT	7
3. PRESENTATION DU 3DSV2	8
3.1 PRINCIPE GENERAL DE FONCTIONNEMENT	8
3.2 PRE-REQUIS.....	8
4. PAYBOX SYSTEM.....	9
4.1 CHANGEMENTS	9
4.2 IMPACTS.....	10
4.3 MODIFICATIONS A APPORTER	11
5. PAYBOX DIRECT	13
5.1 IMPACTS.....	13
5.2 MODIFICATIONS A APPORTER	15
6. SOUSCRIPTION ET TESTS	17
6.1 ELIGIBILITE	17
6.2 CARTES DE TESTS 3DSV2.....	17
6.3 CARTES DE TESTS 3DSV1.....	20

1. INTRODUCTION

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



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

- Multi-canal : la plateforme Paybox accepte différents systèmes d'accès autant physiques (paiement de proximité) que distants (VAD, E-Commerce) :
 - Site web marchand
 - Terminal de Paiement Electronique, ou ligne de caisse d'un magasin ou d'une enseigne
 - Automate de distribution
 - Téléphone mobile ou PDA
 - Centre d'appels, centre de saisie, serveur vocal interactif ...

- Multi-services : la plateforme Paybox gère une multitude de moyens de paiement :
 - cartes bancaires,
 - cartes privatives,
 - cartes de crédit,

Mais elle gère également de nombreux services et applications métiers :

- les cartes cadeaux,
- les cartes de fidélité,
- la gestion de flotte,
- la réservation de véhicules ...

2. OBJET DU DOCUMENT

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

- **PAYBOX SYSTEM** : Paybox System s'interface avec le site marchand Internet ou mobile. Les clients acheteurs sont redirigés automatiquement sur les pages de paiement multilingues hébergées par Verifone. Ces pages sont personnalisables pour les harmoniser avec l'identité graphique du site Marchand. Paybox System répond aux normes de sécurité des paiements par carte sur les sites d'e-commerce en affichant une page TLS et en utilisant le protocole 3-D Secure (si option souscrite).
- **PAYBOX DIRECT (PPPS)** : Paybox Direct assure le traitement des paiements de façon transparente pour les clients acheteurs. L'application de vente du marchand doit collecter les informations sensibles telles que le n° de carte et les transmet à Paybox via un dialogue sécurisé de serveur à serveur.

Paybox Direct est également utilisé pour valider les encaissements des transactions préalablement autorisées via Paybox System, assurer des remboursements et annulations de serveur à serveur. Compléter Paybox System avec Paybox Direct permet au commerçant de gagner en flexibilité en intégrant le pilotage des opérations post-autorisation en mode serveur à serveur depuis son application de vente (ou back-office).
- **PAYBOX DIRECT Plus** : Désigne le service Paybox où l'Application de vente du commerçant demande à Paybox de conserver les données du moyen de paiement. Cette solution s'interface parfaitement en complément de Paybox System ou bien directement en mode serveur à serveur.

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

Le présent document est le manuel d'intégration des attentes liées à la deuxième Directive sur les Service de Paiement (DSP2) et plus particulièrement l'implémentation de l'**authentification 3DSv2** dans la solution Paybox.

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

3. PRESENTATION DU 3DSV2

3.1 PRINCIPE GENERAL DE FONCTIONNEMENT

L'entrée en vigueur de la deuxième Directive européenne sur les Services de Paiements (DSP2) refuse à partir d'avril 2021 les transactions sans authentification ni exemption. L'ensemble des e-commerçants et des transactions doivent employer EMV 3D-Securev2 ou procéder à une demande d'authentification systématique.

Un nouveau protocole d'authentification défini conjointement par le Groupement Carte Bancaire, Visa et Mastercard permet d'obtenir cette authentification sans demander systématiquement un challenge au porteur de la carte – habituellement réalisé par un SMS ou par une connexion à l'application de sa banque.

Le présent document présente les modifications liées à cette réglementation dans le cadre des produits Paybox System et Paybox Direct.

Il s'agit d'un complément aux manuels existants et seules les évolutions par rapport à ces manuels seront décrites.

3.2 PRE-REQUIS

Afin d'être en conformité avec la DSP2, les modifications décrites dans les paragraphes ci-dessous seront nécessaires.

Pour être éligible à la procédure de migration, le marchand devra :

- Utiliser le Back Office Vision pour la visualisation et exploitation de ses transactions.
- Disposer d'un contrat CB2A version 5.5 (ce changement de version est traité entre Verifone et chaque banque acquéreur).

4. PAYBOX SYSTEM

4.1 CHANGEMENTS

La mise en place de la DSP2 s'accompagne des modifications de fonctionnalités suivantes.

4.1.1 Ajout du Soft Decline

Durant la phase de migration, certaines transactions pour lesquelles le porteur de la carte n'aura pas été authentifié pourront être rejetées par un mécanisme de Soft Decline.

Le centre d'autorisation renverra un code erreur spécifique qui sera retourné aux marchands sous la forme 001A1.

Remarque : Pour obtenir ce code en retour d'un appel Paybox System, il sera nécessaire de valoriser le paramètre e dans la variable PBX_RETOUT.

4.1.2 Retrait du débrayage 3D-Secure

La DSP2 impose que les porteurs des transactions soient authentifiés ce qui rend contreproductive la fonctionnalité de débrayage proposée pour les transactions Paybox System par la variable PBX_3DS.

Une fois les contrats configurés pour être compatibles DSP2, cette variable ne sera plus prise en compte pour le 3D-Secure v1 et aucun équivalent ne sera proposé pour le 3D-Secure v2.

4.1.3 Connaître la version de 3D-Secure utilisée

Pour permettre au marchand de savoir si la transaction a été réalisée en 3D-Secure v1 ou v2, un nouveau paramètre « v » est disponible dans la variable PBX_RETOUT.

Lorsque ce paramètre est demandé, la version de 3D-Secure utilisée pour la transaction concernée est retournée dans la réponse faite au marchand.

Attention : A partir d'avril 2021 les transactions sans authentification ni exemption sont refusées. L'ensemble des e-commerçants et des transactions doivent employer EMV 3D-Secure v2 ou procéder à une demande d'authentification systématique.

4.2 IMPACTS

L'ensemble des tentatives de paiement réalisées avec Paybox System sont concernées par l'authentification du porteur.

Avec l'entrée en vigueur de la DSP2, l'authentification du porteur sera attendue par l'émetteur de la carte de paiement lors de chaque tentative de paiement.

4.2.1 3D-Secure v1

Pour permettre l'authentification du porteur sans modification dans l'implémentation du paiement, le marchand devra se rapprocher de sa banque pour obtenir un contrat VADS. Ce contrat devra être transmis à Verifone qui opérera l'enrôlement et la configuration du contrat.

Remarque : Cette méthode impose une action du porteur pour s'identifier (appelée challenge) lors de chaque tentative de paiement (par exemple l'envoi d'un code par SMS).
Ce challenge est une source de **friction lors de la vente.**

Attention : A partir d'avril 2021 les transactions sans authentification ni exemption sont refusées. L'ensemble des e-commerçants et des transactions doivent employer EMV 3D-Secure v2 ou procéder à une demande d'authentification systématique.

4.2.2 3D-Secure v2

Le marchand devra se rapprocher de sa banque pour obtenir un contrat VADS. Ce contrat devra être transmis à Verifone qui opérera l'enrôlement et la configuration du contrat.

Cependant, cette nouvelle version du 3D-Secure ne sera opérationnelle qu'après modification de l'implémentation du marchand telle que décrit dans le paragraphe

4.3 Modifications à apporter.

Remarque : La recommandation de Verifone ainsi que des instances réglementaires françaises (GIE-CB) et européenne (ABE) est de mettre en place le 3D-Secure v2.

4.3 MODIFICATIONS A APPORTER

Ces modifications concernent uniquement l'implémentation du 3D-Secure v2.

4.3.1 PBX_SHOPPINGCART

Format : XML. **Obligatoire.**

Cette variable contiendra un élément XML <shoppingcart> qui sera enrichi dans le futur.

Une seule donnée sera obligatoire pour des raisons protocolaires, le nombre d'articles constituant la commande.

Il sera valorisé dans un champ numérique allant de 1 à 99, sera nommé <totalQuantity> et s'intégrera comme suit :

Exemple :

```
<?xml version="1.0" encoding="utf-8"?>
<shoppingcart>
  <total>
    <totalQuantity>15</totalQuantity>
  </total>
</shoppingcart>
```

4.3.1 PBX_BILLING

Format : XML. **Obligatoire.**

Les informations concernant le porteur de carte et son adresse de facturation.

Nom	Description	Type	Présence
Billing	Balise XML à la racine	XML	O
Address	Balise XML	XML	O
FirstName	Prénom du client	ANP..30 (incluant / - ')	O
LastName	Nom du client	ANP..30 (incluant / - ')	O
Address1	Adresse de facturation	ANS..50	O
Address2	Adresse de facturation	ANS..50	F
ZipCode	Code postal de l'adresse de facturation	ANS..16	F
City	Ville de l'adresse de facturation	ANS..50	O
CountryCode	Code pays de l'adresse de facturation	ANS..3	O

AN : Alpha Numérique sans caractères spéciaux

ANP : Alpha Numérique avec les espaces et caractères accentués

ANS : Alpha Numérique avec caractères spéciaux

N : Numérique uniquement

A : Alphabétique uniquement

O : Obligatoire

C : Conditionnel

F : Facultatif

Exemple :

```
<?xml version="1.0" encoding="utf-8"?>
<Billing>
  <Address>
    <FirstName>Jean</FirstName>
    <LastName>Dupont</LastName>
    <Address1>12 rue Paul Dautier</Address1>
    <ZipCode>78140</ZipCode>
    <City>Vélizy-Villacoublay</City>
    <CountryCode>250</CountryCode>
  </Address>
</Billing>
```

5. PAYBOX DIRECT

5.1 IMPACTS

L'ensemble des tentatives de paiement réalisées avec Paybox Direct sont concernées par l'authentification du porteur.

Avec l'entrée en vigueur de la DSP2, l'authentification du porteur sera attendue par l'émetteur de la carte de paiement lors de chaque tentative de paiement.

5.1.1 3D-Secure v1

Pour permettre l'authentification du porteur, il sera nécessaire d'intégrer à l'implémentation de Paybox Direct les données provenant d'une authentification 3D-Secure.

La réalisation d'une authentification 3D-Secure associée à la tentative de paiement pourra être faite par une implémentation du produit Remote MPI – détail d'implémentation dans le manuel dédié.

Pour permettre le fonctionnement des modifications de son implémentation et donc l'authentification des porteurs, le marchand devra se rapprocher de sa banque pour obtenir un contrat VADS. Ce contrat devra être transmis à Verifone qui opérera l'enrôlement et la configuration du contrat.

Remarque : Cette méthode impose une action du porteur pour s'identifier (appelée challenge) lors de chaque tentative de paiement (par exemple l'envoi d'un code par SMS).
Ce challenge est une source de **friction lors de la vente.**

Attention : A partir d'avril 2021 les transactions sans authentification ni exemption sont refusées. L'ensemble des e-commerçants et des transactions doivent employer EMV 3D-Secure v2 ou procéder à une demande d'authentification systématique.

5.1.2 3D-Secure v2

Pour permettre l'authentification du porteur, il sera nécessaire d'intégrer à l'implémentation de Paybox Direct les données provenant d'une authentification 3D-Secure.

Pour simplifier la transition d'une implémentation 3D-Secure v1 vers une implémentation 3D-Secure v2 ; la réalisation d'une authentification 3D-Secure v2 associée à la tentative de paiement pourra également être faite par une implémentation du produit Remote MPI.

Cette nouvelle version du 3D-Secure ne sera opérationnelle qu'après certaines modifications à apporter à l'implémentation Remote MPI. Le détail des ajustements est listé dans le paragraphe **5.2 Modifications à apporter**.

Pour permettre le fonctionnement des modifications de son implémentation et donc l'authentification des porteurs, le marchand devra se rapprocher de sa banque pour obtenir un contrat VADS. Ce contrat devra être transmis à Verifone qui opérera l'enrôlement et la configuration du contrat.

Remarque : La recommandation de Verifone ainsi que des instances réglementaires françaises (GIE-CB) et européenne (ABE) est de mettre en place le 3D-Secure v2.

5.2 MODIFICATIONS A APPORTER

Ces modifications concernent uniquement l'implémentation du 3D-Secure v2.

5.2.1 Trame à modifier

Les modifications concernent l'étape 3 de la cinématique Remote MPI, l'appel à l'iFrame `remoteMPI.cgi`.

La structure de l'appel sera conservée, mais différentes données devront y être ajoutées pour permettre le fonctionnement du 3D-Secure v2.

Remarque : Les données spécifiques nécessaires à l'affichage des pages d'authentification 3D-Secure v2 seront obtenues par un JavaScript qui sera intégré à la page hébergée par Verifone sans action côté marchand.

5.2.2 Données à ajouter

Liste de données à ajouter dans l'appel à la page `remoteMPI.cgi`.

Nom	Description	Type	Présence
EmailPorteur	Email du porteur de carte	AN.6.120 (incluant @ et .)	O
TypeCarte	Type de carte choisi par le porteur	Parmis les valeurs suivantes : CB, VISA, MASTERCARD, ELECTRON, MAESTRO, E_CARD, VPAY	F
FirstName	Prénom du client	ANP..30 (incluant / - ')	O
LastName	Nom du client	ANP..30 (incluant / - ')	O
Address1	Adresse de facturation	ANS..50	O
Address2	Adresse de facturation	ANS..50	F
ZipCode	Code postal de l'adresse de facturation	ANS..16	F
City	Ville de l'adresse de facturation	ANS..50	O
CountryCode	Code pays de l'adresse de facturation	ANS..3	O
TotalQuantity	Nombre d'articles composant la commande.	N..2	O

AN : Alpha Numérique sans caractères spéciaux

ANP : Alpha Numérique avec les espaces et caractères accentués

ANS : Alpha Numérique avec caractères spéciaux

N : Numérique uniquement

A : Alphanumérique uniquement

O : Obligatoire
C : Conditionnel
F : Facultatif

Remarque : Si le TypeCarte fourni n'est pas reconnu, cette valeur sera assignée selon les préférences définies par la configuration du compte marchand - CB par défaut.

5.2.3 Réalisation de l'appel à Paybox Direct

L'implémentation d'une authentification par le RemoteMPI se termine par la transmission du contexte 3D-Secure dans l'appel Paybox Direct. Cette transmission est indispensable car nécessaire à la réalisation de la demande d'autorisation.

Paybox Direct prévoit deux modes permettant de transmettre le contexte 3D-Secure.

- L'envoi de la variable ID3D

Ou

- L'envoi de l'ensemble des variables suivantes ; 3DSTATUS, 3DENROLLED, 3DECI, 3DERROR, 3DXID, 3DCAVV, 3DCAVVALGO et 3DSIGNVAL.

Dans le cadre d'une authentification 3D-Secure v1, les deux modes sont supportés, mais les spécificités d'une implémentation 3D-Secure v2 sont uniquement compatibles avec l'envoi de la variable ID3D.

Attention : Dans le cadre d'une authentification 3D-Secure v2, la transmission du contexte pourra se faire uniquement par l'envoi de la variable ID3D. L'envoi des variables 3DSTATUS, 3DENROLLED, 3DECI, 3DERROR, 3DXID, 3DCAVV, 3DCAVVALGO et 3DSIGNVAL ne permettra pas la réalisation d'un paiement 3D-Secure v2.

6. SOUSCRIPTION ET TESTS

Le suivi de la réglementation fait partie intégrante des activités Verifone et le fonctionnement habituel est maintenu, le commercial en contact avec le marchand reste le point d'entrée privilégié pour modifier la configuration du ou des contrats.

6.1 ELIGIBILITE

La réalisation des tests en environnement de recette pourra se faire sur les contrats génériques mis à disposition par Verifone, mais également sur le contrat du marchand après la migration de celui-ci.

Attention : Un contrat n'ayant pas été migré dans les interfaces Verifone ne permettra pas la réalisation de tests 3DSv2.

Remarque : Les tests réalisés sur la plateforme de Recette seront réalisés par le biais d'un simulateur dont les différents comportements seront déclenchés par la saisie des numéros de cartes ci-dessous.

6.2 CARTES DE TESTS 3DSV2

6.2.1 Cas de test Visa

Authentification réussie :

- Numéro de carte : 4000000000001091
- Date de validité : Janvier de l'année suivante

Authentification Frictionless réussie :

- Numéro de carte : 4000000000001000
- Date de validité : Janvier de l'année suivante

Authentification échouée :

- Numéro de carte : 4000000000001091
- Date de validité : Janvier de l'année suivante

Authentification Frictionless échouée :

- Numéro de carte : 4000000000001018
- Date de validité : Janvier de l'année suivante

Authentification status Attempt:

- Numéro de carte : 4000000000001026
- Date de validité : Janvier de l'année suivante

Erreur pendant la recherche de la carte :

- Numéro de carte : 4000000000001067
- Date de validité : Janvier de l'année suivante

Authentification indisponible :

- Numéro de carte : 4000000000001117
- Date de validité : Janvier de l'année suivante

Authentification en erreur :

- Numéro de carte : 4000000000001125
- Date de validité : Janvier de l'année suivante

6.2.2 Cas de test MasterCard

Authentification réussie :

- Numéro de carte : 5200000000001096
- Date de validité : Janvier de l'année suivante

Authentification Frictionless réussie :

- Numéro de carte : 5200000000001005
- Date de validité : Janvier de l'année suivante

Authentification échouée :

- Numéro de carte : 5200000000001104
- Date de validité : Janvier de l'année suivante

Authentification Frictionless échouée :

- Numéro de carte : 5200000000001013
- Date de validité : Janvier de l'année suivante

Authentification status Attempt:

- Numéro de carte : 5200000000001021
- Date de validité : Janvier de l'année suivante

Erreur pendant la recherche de la carte :

- Numéro de carte : 5200000000001062
- Date de validité : Janvier de l'année suivante

Authentification indisponible :

- Numéro de carte : 5200000000001112
- Date de validité : Janvier de l'année suivante

Authentification en erreur :

- Numéro de carte : 5200000000001120
- Date de validité : Janvier de l'année suivante

6.3 CARTES DE TESTS 3DSV1

Remarque : L'utilisation de 3DSv1 satisfait aux exigences de la DSP2, mais ne peut pas être une solution long terme. Cette version du protocole sera arrêté dans le deuxième semestre 2021.

6.3.1 Cas de test Visa

Authentification réussie :

- Numéro de carte : 4000000000000002
- Date de validité : Janvier de l'année suivante

Authentification échouée :

- Numéro de carte : 4000000000000028
- Date de validité : Janvier de l'année suivante

Authentification status Attempt:

- Numéro de carte : 4000000000000101
- Date de validité : Janvier de l'année suivante

Porteur non enrôlé :

- Numéro de carte : 4000000000000051
- Date de validité : Janvier de l'année suivante

Authentification indisponible :

- Numéro de carte : 4000000000000069
- Date de validité : Janvier de l'année suivante

Authentification en erreur :

- Numéro de carte : 4000000000000093
- Date de validité : Janvier de l'année suivante

6.3.2 Cas de test Mastercard

Authentification réussie :

- Numéro de carte : 5200000000000007
- Date de validité : Janvier de l'année suivante

Authentification échouée :

- Numéro de carte : 5200000000000023
- Date de validité : Janvier de l'année suivante

Authentification status Attempt:

- Numéro de carte : 5200000000000908
- Date de validité : Janvier de l'année suivante

Porteur non enrôlé :

- Numéro de carte : 5200000000000056
- Date de validité : Janvier de l'année suivante

Authentification indisponible :

- Numéro de carte : 5200000000000064
- Date de validité : Janvier de l'année suivante

Authentification en erreur :

- Numéro de carte : 5200000000000098
- Date de validité : Janvier de l'année suivante