Guide d'intégration technique général

Guide d’integration technique
Guide d'intégration
Version 1.0
Date 25/03/2020

Table des matières

Historique des versions

Date	Nom	Modification
25/03/2020	Peter Posse	Version originale

Acronymes et abréviations

Formats des données :

a	alphabétique

as	alphabétique avec caractères spéciaux
n	numérique
an	alphanumérique
ans	alphanumérique avec caractères spéciaux
ns	numérique avec caractères spéciaux
bool	expression booléenne (true ou false)
3	longueur fixe avec 3 chiffres/caractères
..3	longueur variable avec maximum 3 chiffres/caractères
enum	énumération de valeurs admissibles
dttm	Date et heure ISO (AAAA-MM-JJThh:mm:ss)

Abréviations :

CND	condition
M	obligatoire (mandatory en anglais)
O	optionnel
C	conditionnel

Remarque : Veuillez noter que les noms des paramètres peuvent être en majuscules ou en minuscules.

Introduction

La solution de paiement Axepta BNP Paribas accepte les ordres de paiement, traite les données et exécute les transactions de paiement du commerçant en toute sécurité.

Ce manuel décrit l'intégration de la solution de paiement Axepta BNP Paribas au système du commerçant et s'adresse aux développeurs et aux responsables techniques.

Principes majeurs de la programmation de la solution

Afin d'envoyer les ordres de paiement à la solution de paiement Axepta BNP Paribas, le commerçant:

- Se connecte via Internet à la solution de paiement Axepta Online
- Envoie les données de paiement requises dans un format homogène

Pour garantir la compatibilité avec **tous les langages de programmation** et **tous les systèmes d'exploitation** (Linux, Unix, Windows), la solution de paiement Axepta BNP Paribas élimine la nécessité d'avoir recours à un logiciel de compatibilité sur le serveur du commerçant. L'installation logicielle entraîne généralement des problèmes avec les versions des systèmes d'exploitation ou les règles de sécurité.

Quelle que soit la méthode de paiement choisie, les paramètres envoyés sont toujours les mêmes. Cela afin que toutes les méthodes de paiement fonctionnent de la même manière et ne nécessitent aucun effort supplémentaire.

Afin de garantir le stockage sécurisé des données de paiement, les réseaux ont élaboré un programme de sécurité avec la certification de sécurité **PCI** (Payment Card Industry). L'emplacement où les données de paiement sont enregistrées est crucial pour la sécurité des paiements sur internet.

Intégration de la solution de paiement Axepta Online

La solution de paiement propose **4 options d'intégration** différentes :

- Paiement via **le formulaire de la page de paiement**
- Paiement via la connexion **server-to-server**
- Paiement par **batch**
- Paiement via **In-App** (SDK Mobile)

	1.Formulaire de page de paiement		2.Server-to-Server	3.Batch		4.In-app (SDK Mobile)
Mode d' intégration	Page de paiement **hébergée par BNP Paribas**	Page de paiement hébergée **par le commerçant**	Connexion Server-to-server	Automatique (Via transfert sFTP)	Manuel (Via Back office)	SDK Hybride (Natif et Webview en fonction du moyen de paiement utilisé)
Hébergement de la page	Serveur Axepta BNP Paribas	Serveur du commerçant		NA	NA	Serveur Axepta BNP Paribas
Stockage des données	Serveur Axepta BNP Paribas		Serveur du commerçant	Serveur Axepta BNP Paribas	Serveur Axepta BNP Paribas	Serveur Axepta BNP Paribas
Format des données	Paramètres d'URL (Format NVP: Name-value-pairs)	Paramètres de saisie (Format NVP: Name-value-pairs)	Paramètres d'URL (Format NVP: Name-value-pairs)	Fichiers CSV (Format .dat)	Fichiers CSV (Format .dat)	Paramètres de saisie au SDK
Transfert des données	Via HTTP GET ou POST	Via HTTP POST	Via HTTP POST	Via sFTP	Via backoffice (Fonction upload)	Via HTTP POST
Niveau PCI-DSS	PCI- SAQ A (22 questions)	SAQ A-EP (191 questions)	PCI DSS Full (329 questions)	PCI- SAQ A (Tant qu'aucun numéro de carte réelle n'est utilisé)	PCI- SAQ A (Tant qu'aucun numéro de carte réelle n'est utilisé)	PCI- SAQ A (22 questions)

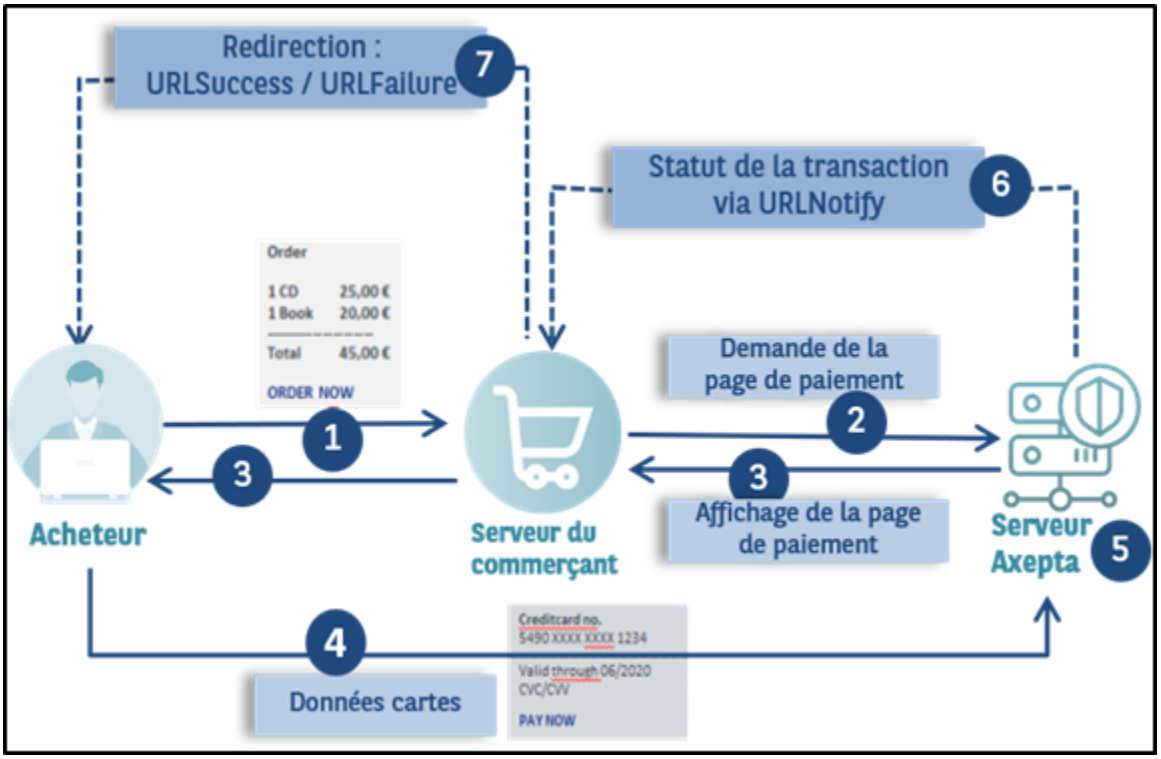
Formulaires de la page de paiement

Le formulaire de la page de paiement et les données de paiement sont hébergés par Axepta

Cette option est la méthode la plus simple et la plus rapide pour intégrer la solution.

La solution de paiement fournit des formulaires **HTML** avec chiffrement **TLS** et certifiés **SSL**. Le site web doit uniquement appeler le « formulaire HTML » de la solution de paiement pour le faire apparaître soit en **redirection complète**, soit en **iFrame**, soit en **lightbox** (pop-up). Ce choix dépend du commerçant. Ensuite, les acheteurs saisissent leurs informations de paiement via ce formulaire HTML. Ces données seront transférées via une requête **HTTP POST** en tant que paramètres **d'URL** (**URL : payssl.aspx**).

Le commerçant doit uniquement se conformer au formulaire **PCI- SAQ A**.

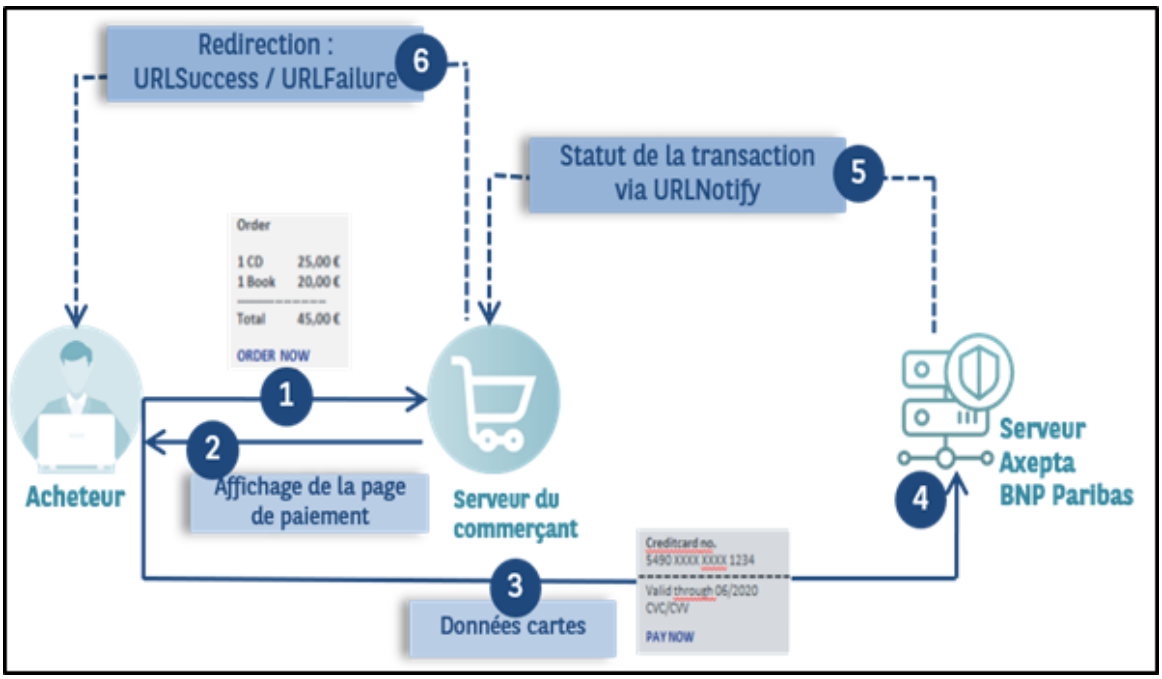


Le formulaire de la page de paiement est héberge par le commerçant et les données de paiement sont hébergés par Axepta

Cette option (appelée également « Silent order post » ou « Direct post ») donne plus de contrôle au commerçant puisque c'est à lui d'afficher directement le formulaire de la page de paiement sur son site. Le commerçant peut alors développer son propre modèle de page de paiement et l' héberger sur son serveur. Il va afficher la page de paiement lorsque l'acheteur validera son panier et envoyer les données de paiement directement au serveur d'AXEPTA BNP Paribas.

Ces données peuvent être capturées sur le site web du commerçant sans être traitées par le serveur du commerçant, d'où l'intérêt d'envoyer la requête **POST** en mode **silencieux** vers le serveur Axepta BNP PARIBAS (**URL : paynow.aspx)** comprenant les données en tant que paramètres de saisie du formulaire et non pas en tant que paramètres d'URL comme c'est le cas lors de l'appel payssl.aspx.

Afin d'utiliser cette option, le commerçant doit respecter l'exigence PCI relative au **SAQ A-EP**.



A noter : Les tentatives de reconnexion automatique à la solution de paiement doivent être désactivées en utilisant le mode « paynow » car la solution de paiement ne peut pas renvoyer l'acheteur vers la page de paiement précédente du commerçant. Veuillez contacter le support de BNP Paribas pour effectuer la désactivation.

Demander le formulaire de page de paiement BNP Paribas

La demande d'un formulaire de la solution de paiement débute avec la composition correcte des paramètres comprenant une clé et une valeur séparées par le signe égal (**=**). Il s'agit de la méthode **NVP** (Name-Value-Pairs) :

```
MerchantID=YourMerchantID
```

Tous les paramètres sont assemblés pour former une chaîne de caractères et séparés par le caractère **&** :

```
Amount=100&Currency=EUR&TransID=12345
```

Remarque : les caractères « **=** » et « **&** » étant utilisés en tant que caractères de séparation, ils ne peuvent pas être transmis comme des valeurs. Toutes les valeurs que vous transmettez sans chiffrement Blowfish doivent être encodées au format URL.

Une chaîne de caractères correcte pour la solution de paiement contient trois paramètres de base : **MerchantID** (Identifiant du commerçant), **Len** (Longueur) et **Data** (Données). Les paramètres **MerchantID** et **Len** ne sont pas chiffrés. Seul le paramètre **Data** est chiffré avec la méthode **Blowfish** :

```
MerchantID=YourMerchantID&Len=67&Data=0A67FE96a65d384350F50FF1
```

Le paramètre **Data** (Données) comprend les détails de paiement essentiels comme le montant et la devise.

Le paramètre **Len** (Longueur) est très important pour le chiffrement, car il contient la longueur de la chaîne de caractères non chiffrée dans le paramètre **Data**. La quantité de données à chiffrer étant multipliée par 8 dans le cas du chiffrement Blowfish, la longueur correcte de la chaîne de caractères doit être connue pour le déchiffrement, sans quoi d'autres caractères non prévus apparaissent à la fin de la chaîne de caractères.

Les paramètres sont transmis via **HTTPS POST** ou **HTTPS GET**. La méthode de transmission recommandée est **HTTPS POST**, car la chaîne de caractères du paramètre dans le cas de GET, jointe à l'URL, est limitée à 2 048 octets selon le navigateur, contrairement à la méthode POST qui n' est pas limitée par la taille de l'URL.

Remarque : la longueur maximale d'une requête de paiement est limitée à 5120 caractères. Si vous devez utiliser des chaînes plus longues, contactez le Support BNP Paribas.

Le développement d'une requête de paiement, sans chiffrement, pourrait être représenté comme suit :

```
MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=https://www.shop.fr/ok.
html&URLFailure=https://www.shop.frfr/failed.html&URLNotify=https://www.shop.com/notify.cgi&OrderDesc=My purchase
```

Remarque : une valeur doit être attribuée à chaque paramètre. Ne transmettez pas de paramètres vides, car cela peut entraîner l'échec du paiement.

Cette chaîne de caractères est ensuite chiffrée et transmise en tant que paramètre Data (Données) et se présente comme suit :

```
<A href="https://paymentpage.axepta.bnpparibas/payssl.aspx?
MerchantID=YourMerchantID&Len=162&Data=E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D34DF217E27FA2E194B9968DE9ABAE3
B1F44B5485EFE3EF2597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B160252A03
7135421FD0CE092C174A7D1D63517BD45099AC2B682F5E3CD2C942A6F0E741A833C0&Background=https://www.myshop.fr/grachic
/background.jpg">Amount</A>
```

Remarque : Les paramètres sont transmis non chiffrés pour garantir la bonne mise en page du formulaire.

Un formulaire HTML est produit pour HTTPS POST et tous les paramètres sont transmis en tant que champs masqués. Seul le bouton « **Payer »** est visible pour le client :

```
<FORM method="POST" action="https://paymentpage.axepta.bnpparibas/payssl.aspx">

    <INPUT type="hidden" name="MerchantID" value="YourMerchantID">

    <INPUT type="hidden" name="Len"       value="162">

    <INPUT type="hidden" name="Data"      value="
E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D34DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340
CDFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B160252A037135421FD0CE092C174A7D1D63517BD4509
9AC2B682F5E3CD2C942A6F0E741A833C0">

    <INPUT type="hidden" name="Background"

value="https://www.myshnop.fr/graphic/background.jpg">

    <INPUT type="submit" name="Pay"     value="Pay">

</FORM>
```

Authentification Hash MAC

Pour vous protéger de toute manipulation non autorisée de vos transactions de paiement, la solution de paiement AXEPTA BNP Paribas vérifie si votre requête de paiement est **authentique** grâce à l'authentification **HMAC** (Hash Message Authentication Code). Vous devrez donc transférer une valeur HMAC à la solution de paiement pour chaque transaction dans le paramètre **MAC**.

NB: il existe une méthode de décodage pour chaque méthode d'encodage et quiconque possédant la clé correcte ou brisant le chiffrement peut lire et manipuler les données. Par conséquent, aucune méthode de chiffrement n'est sûre à 100 %. Cependant avec la procédure Hash en revanche, le décodage est impossible et la valeur Hash permet de confirmer formellement l'authenticité du message.

La solution de paiement utilise un code HMAC (Hash Message Authentication Code) pour vérifier l'authenticité de vos paiements. L'algorithme MAC SHA-256 est utilisé avec une clé de 32 chiffres (256 bits). Un mot de passe supplémentaire renforce la sécurité de la procédure HMAC.

Le tableau suivant décrit la méthode de génération des valeurs Hash pour votre paiement :

Étape	Tâche
1	Vous allez recevoir le code HMAC par mail
2	La valeur HMAC est calculée grâce au code et à différentes valeurs de paramétrage. Pour le calcul, les paramètres PayID (Identifiant du paiement), TransID (Identifiant du transfert), MerchantID (Identifiant du commerçant), Amount (Montant) et Currency (Devise) sont utilisés et séparés par des astérisques : PayID*TransID*MerchantID*Amount*Currency Remarque : si une transaction ne prend pas en charge tous ces paramètres, vous pouvez tout simplement omettre la valeur manquante. Par exemple, la première transaction (ci-dessous exemple 1) ne comprend pas le paramètre PayID (Identifiant de paiement). Vous n'avez donc pas à le transférer. L'identifiant du paiement (PayID) est un composant du calcul Hash dans les transactions (exemple 2 et 3): Exemple 1, sans identifiant de paiement PayID (ex. lors de l'autorisation) : *B456Ref890*YourMerchantID*9900*EUR Exemple 2, avec identifiant de paiement PayID (ex. lors de la capture) : 1237890*B456Ref890*YourMerchantID*9900*EUR Exemple 3, sans identifiant TransID : 1237890**YourMerchantID*9900*EUR
3	Utilisez l'algorithme MAC SHA-256, pris en charge par la grande majorité des langages de programmation, afin de calculer la valeur Hash avec le mot de passe et les valeurs de paramétrage.
4	Utilisez le paramètre Mac pour transférer la valeur Hash avec encodage en hexadécimal à la solution de paiement avec chaque transaction dans le champ de données encodées.

Remarque : Si le paramètre MAC a été transféré avec la première transaction (demande d'autorisation), il est obligatoire pour toutes les transactions suivantes (ex. capture, remboursement, etc).

Important : La solution de paiement rejette immédiatement les transactions avec des valeurs HMAC erronées ou manquantes sans autre traitement, car il s'agit probablement d'un piratage. Par conséquent, les transactions que la solution de paiement rejette avec les codes d'erreur 20100044 ou 20120044 n'apparaissent pas dans le back office Axepta BNP Paribas (Se référer au document regroupant les codes retours).

Quelques exemples de codes HMAC

1. Requête sans PayID:

MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=https://www.shop.fr/ok.html&URLFailure=https://www.shop.de/failed.html&OrderDesc=My purchase

Chaine de caractères pour générer un code MAC :

*100000001*Test*11*EUR

Requête avec un code MAC :

MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=https://www.shop.fr/ok.html&URLFailure=https://www.shop.de/failed.html&OrderDesc=My purchase&MAC=A0E3A8BB9473CF4D3F91181E0859650A9AF3F4AD0AE1E839AC7B750247A2E947

2. Requête sans TransID:

MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD

Chaine de caractères pour générer un code MAC :

8ee4e922c39446ac9ee66095a4a4b475**Test*100*USD

Requête avec un code MAC :

MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD&MAC=F1EB4A8BB9473CF4D3F91181F0859659A9AF3F4AD0AE1E839AC7B750247A2D636

Le site web du commerçant doit vérifier que la notification de paiement provient réellement de BNP Paribas. En effet, un fraudeur peut initialiser une transaction et falsifier cette notification. Par conséquent, le système du commerçant doit le faire automatiquement.

Actuellement, la requête de notification est uniquement chiffrée. Toutefois, ce chiffrement ne garantit pas l'authenticité d'un message. Cela garantit uniquement qu'un message ne peut pas être écouté. Il est donc impératif pour le commerçant d'utiliser le paramètre de réponse MAC, basé sur le même algorithme de saisie MAC (seuls les paramètres de données seront différents).

Le schéma de données suivant s'applique ici pour la génération du code Hash :

*PayID*TransID*MerchantID*Status*Code*

Le paramètre MAC est uniquement retourné à l'URL Success (Réussite) ou Failure (Échec), et Notify (Notification).

Notification de la boutique

Après l'exécution du paiement, la solution de paiement notifie la boutique du résultat du paiement. Pour ce faire, la solution de paiement appelle **URLNotify** via HTTP POST. Il s'agit d'une communication **entièrement distincte** de la connexion d'origine entre la boutique, l'acheteur et la solution de paiement. Les paramètres sont transmis dans le corps HTTP en tant que chaîne de paramètre en chiffrement Blowfish. Type de contenu : **application/x-www-form-urlencoded; charset=iso-8859-1**. Par conséquent, les valeurs standards pour l'analyse du formulaire HTML sont utilisées.

Remarque : l'appel Notify est autorisé uniquement via le Port 443 (TLS) pour des raisons de sécurité.

Si l'**URLNotify** de la boutique n'est pas accessible (p. ex. statut HTTP 500/404), la notification est répétée 8 fois. Dans ce cas, le commerçant devra se référer au statut de la demande de transaction (**URLSuccess, URLFailure**).

Répétition	Temps d'attente	Durée après la 1re notification
0	instantanément	0
1	00:01 h	00:01 h
2	00:08 h	00:09 h

3	00:27 h	00:36 h
4	01:04 h	01:40 h
5	02:05 h	03:45 h
6	03:36 h	07:21 h
7	05:43 h	13:04 h
8	08:32 h	21:36 h

Durée avant répétition de la notification calculée après l'échec de la première tentative

Remarque : les paramètres avec **encodage URL** sont transmis dans des key value pairs (Key1=Value1&Key2=Value2). De nouveaux paramètres peuvent être ajoutés à tout moment, sans préavis. Par conséquent, nous recommandons l'utilisation du nom du paramètre pour l'analyse, et **non** de l'ordre (la commande) car celui-ci peut changer à tout moment. N'utilisez pas des caractères sensibles à la casse pour ces paramètres, car cela peut être modifié à tout moment. Nous recommandons par exemple de passer tous les caractères en minuscules, et de poursuivre avec des minuscules.

Pour en savoir plus, rendez-vous sur : www.w3.org/MarkUp/html-spec/html-spec_8.html#SEC8.2.1

Redirection du client vers le site web du commerçant

Lorsque le paiement est effectué, le client est redirigé via HTTP GET vers la boutique. La solution de paiement retourne ensuite un statut HTTP 302 (objet déplacé) et joint le statut du paiement en tant que paramètre avec chiffrement Blowfish à **URLSuccess** ou **URLFailure**. Les URLs (Success et Failure) sont des pages spécifiées par le commerçant. Axepta BNP Paribas redirige l'acheteur vers l'une de ces pages en fonction du résultat : URLSuccess si le paiement est réussi et URLFailure si le paiement est échoué.

Tests

Votre compte reste en mode de test jusqu'à ce que la configuration de ce dernier soit terminée : les paiements par carte sont autorisés mais il n'y a pas encore de flux d'argent puisque la solution de paiement n'exécute pas de captures.

Remarque : en mode test, veillez à n'utiliser que des petits montants entre 0,11 et 2 euros car les autorisations de carte sont authentiques, même en mode test, et réduisent la limite de votre carte. Si vous utilisez des montants plus importants et que vous atteignez la limite de carte, votre carte ne fonctionnera pas temporairement.

En cas de paiements réussis, la solution de paiement retourne la valeur zéro dans le paramètre Code. Si un paiement échoue, le paramètre Code est supérieur à zéro et s'explique de plusieurs manières : une date d'expiration incorrecte, une limite de carte dépassée... Vous trouverez une liste complète des codes d'erreur dans le fichier Excel correspondant.

Si vous souhaitez tester les différents cas d'erreur, la solution de paiement vous permet de simuler les codes d'erreur souhaités. Pour simuler une erreur, transmettez le mot-clé Test dans le paramètre **OrderDesc** suivi du code d'erreur détaillé à quatre chiffres, par ex. « Test:0110 » pour simuler une carte arrivée à expiration. La solution de paiement retourne alors le code d'erreur détaillé à quatre chiffres ainsi que les paramètres de réponse correspondants.

Cas de test avec délai d'attente (Timeout)

Un paiement par carte est normalement exécuté en une à deux secondes. Dans certains cas, les paiements peuvent être interrompus en raison de longs délais de traitement dans le réseau bancaire. La solution de paiement met fin aux paiements par carte après 90 secondes. Si vous souhaitez un délai d'attente plus court, notre équipe Support peut configurer ce délai.

Connexion « Server-to-Server »

Le formulaire de la page de paiement et les données de paiement sont hébergés par le commerçant (Server-to-Server)

L'option server-to-server (également appelée machine-to-machine) signifie que la page de paiement du commerçant est entièrement hébergée sur son serveur, et toutes les données de paiement y sont collectées également.

Lorsque le commerçant souhaite concevoir ses propres formulaires pour la saisie des données de paiement, il peut exécuter ses transactions en **arrière-plan** via une **connexion serveur-to-serveur**. Dans ce cas, le système du commerçant **enregistre** les détails du paiement, puis crée une **connexion réseau (socket) TLS** au serveur de la solution de paiement, et envoie ces données afin d'exécuter le paiement. Dans cette variante, le système du commerçant contrôle la communication avec la solution de paiement (cela implique un développement plus poussé comparé aux formulaires de la solution de paiement qui exécutera automatiquement les paiements pour le commerçant).

Le commerçant doit obtenir une certification PCI DSS complète (niveau PCI le plus élevé).

Remarque : Veuillez noter que pour un paiement unique (PayID unique), il n'est pas possible de transmettre des requêtes multiples simultanément, il vaut mieux attendre quelques secondes entre deux requêtes d'un même paiement (PayID).

Execution d'un paiement via une connexion Serveur-to-Serveur

La requête pour un paiement débute avec la combinaison correcte des paramètres, comprenant une clé et une valeur séparées par un signe égal (=). Il s'agit des paires nom-valeur (NVP) :

```
MerchantID=YourMerchantID
```

Tous les paramètres sont assemblés pour former une chaîne de caractères et séparés par le caractère **&**:

```
Amount=100&Currency=EUR&TransID=12345
```

Remarque : les caractères « **=** » et « **&** » étant utilisés en tant que caractères de séparation, ils ne peuvent pas être transmis comme des valeurs. Toutes les valeurs que vous transmettez sans chiffrement Blowfish doivent être encodées au format URL.

Une chaîne de caractères correcte pour la solution de paiement contient trois paramètres de base : **MerchantID** (Identifiant du commerçant), **Len** (Longueur) et **Data** (Données). Les paramètres **MerchantID** et **Len** ne sont pas chiffrés. Seul le paramètre **Data** est chiffré avec la méthode **Blowfish** :

```
MerchantID=YourMerchantID&Len=67&Data=0A67FE96a65d384350F50FF1
```

Le paramètre **Data** (Données) comprend les détails de paiement essentiels comme le montant et la devise.

Le paramètre **Len** (Longueur) est très important pour le chiffrement, car il contient la longueur de la chaîne de caractères non chiffrée dans le paramètre **Data**. La quantité de données à chiffrer étant multipliée par 8 dans le cas du chiffrement Blowfish, la longueur correcte de la chaîne de caractères doit être connue pour le déchiffrement, sans quoi d'autres caractères non prévus apparaissent à la fin de la chaîne de caractères.

L'exemple ci-dessous illustre une requête de paiement non chiffrée :

```
MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&OrderDesc=My
purchase&CCNr=1111333355557777&CCCVC=123&CCExpiry=200407&CCBrand=VISA
```

Remarque : veuillez noter qu'une valeur doit être attribuée à chaque paramètre. Ne transmettez pas de paramètres vides pour éviter l'échec du paiement.

La chaîne de caractères représentant la requête chiffrée avec la méthode Blowfish est la suivante :

```
MerchantID=YourMerchantID&Len=140&Data=D622C5FE7414F73539A1852C2CE7AA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B1602564DBF2C3C75173A62C484962A247B8A91EA7A544ADCF2A037135421FD0CE092C174A7D1D63517BD45099AC2B682F5E3CD2C942A6F0E741A833C
```

Afin de procéder aux paiements via une connexion server-to-server, ouvrez une connexion réseau (socket) TLS avec la solution de paiement et transférez la chaîne de caractères générée sur l'URL suivante :

```
https://paymentpage.axepta.bnpparibas/direct.aspx
```

Dès que la connexion réseau (socket) TLS est établie, une requête HTTP POST version 1.1 normale est effectuée. Dans ce cas, les champs suivants sont spécifiés dans l'en-tête HTTP :

Champ	Valeur
Host (Hôte)	paymentpage.axepta.bnpparibas
Connection (Connexion)	Close (Fermée)
Content-type (Type de contenu)	Application/x-www-form-urlencoded
Content-length (Longueur du contenu)	Longueur de la chaîne de caractères transférée vers le Http-Body (corps http)
Charset (Jeu de caractères)	UTF-8

Le corps HTTP (HTTP Body) contient la chaîne de caractères du paramètre. Les valeurs doivent être soumises en tant que paramètres avec encodage URL. L'exemple suivant est un paiement par carte :

```
POST /direct.aspx HTTP/1.1

Host: paymentpage.axepta.bnpparibas

Connection: Close

Content-type: application/x-www-form-urlencoded

Content-Length: 287


MerchantID=YourMerchantID&Len=162&Data=E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D3E876F52CBECF59EC63E9B8AA0130FA92F65964E3EEE74DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B1602564DBF2C3C75173A62C484962A247B8A91EA7A5
```

Remarque : la longueur maximale d'une requête de paiement est limitée à 5120 caractères. Si vous devez utiliser des chaînes plus longues, contactez le Support BNP Paribas.

L'exemple suivant montre une réponse type de la solution de paiement. La solution de paiement écrit les données chiffrées en Blowfish sur le socket :

```
HTTP/1.0 200 OK

Connection: Close

Content-type: text/plain

Content-Length: 228


Len=125&Data=ECF59EC63E9BEE74DF217E27FA2E194B92597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E233ACDBE5EF98E1692B1602564DBF2C3C75173A62C484962A247B8A91EA7A544
```

La réponse déchiffrée, de la solution de paiement, dans le paramètre **Data** (Données) se présente comme suit :

```
PayID=a234b678e01f34567090e23d567890ce&XID=50f35e768edf34c4e090e23d567890ce&TransID=100000001&Status=AUTHORIZED&Description=AUTHORIZED&Code=00000000
```

Il s'agit d'une communication synchrone, de façon à ce que la connexion « socket » reste ouverte jusqu'à ce que la solution de paiement ait fourni la réponse. Si une requête n'obtient pas de réponse dans les 120 secondes, la solution de paiement peut émettre un message d'expiration.

Remarque : les paramètres **URL-encoded** sont transmis dans des paires « key-value » (Key1=Value1&Key2=Value2). De nouveaux paramètres peuvent être ajoutés à tout moment, sans préavis. Par conséquent, nous recommandons l'utilisation du nom du paramètre pour l'analyse, et non de l' ordre car celui-ci peut changer à tout moment. N'utilisez pas des caractères sensibles à la casse (sensitive case) pour les paramètres, car cela peut être modifié à tout moment.

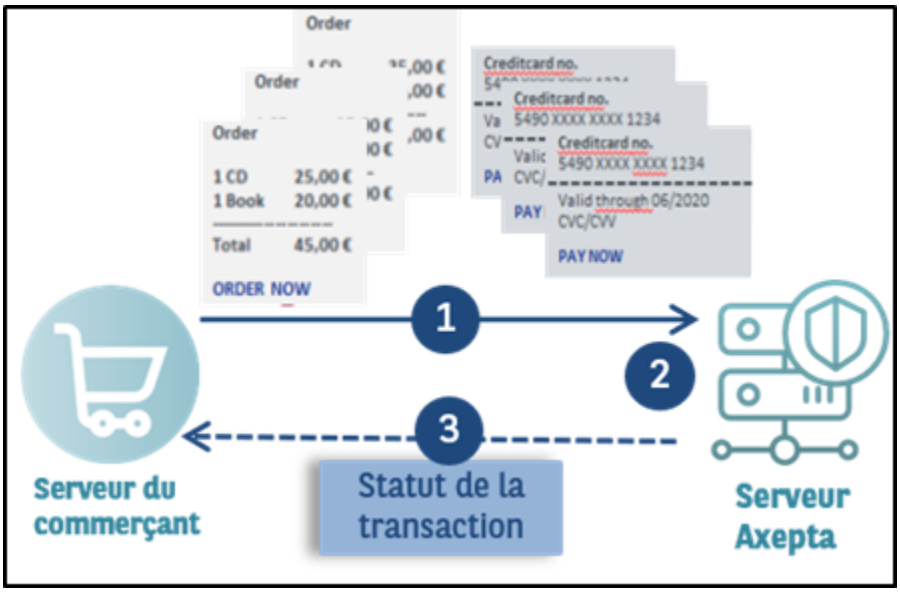
Pour en savoir plus, rendez-vous sur :

www.w3.org/MarkUp/html-spec/html-spec_8.html#SEC8.2.1

Fichiers Batch

Le paiement via Batch consiste à transférer les données des transactions collectées des clients vers le serveur Axepta BNP Paribas sous forme de fichiers formatés. Le transfert peut se faire :

- **Manuellement** via le back-office de BNP Paribas. (Se référer à la documentation Backoffice)
- **Automatiquement** via un protocole de transfert sécurisé (sFTP).



Lors de ce processus, vous associez les données des transactions (comme l'identifiant, le montant et la devise) dans un fichier batch que vous transmettez ultérieurement à la solution de paiement. La solution de paiement procède ensuite aux paiements et enregistre le statut de transaction dans le fichier batch de retour. Après traitement, le commerçant peut télécharger le fichier batch avec les détails sur le statut de la transaction.

L'accès sFTP pour le transfert du fichier batch doit être demandé à l'Assistance BNP Paribas.

Les fichiers batch doivent être correctement **structurés** pour que la solution de paiement puisse les traiter.

Nom des fichiers Batch

Le nom d'un nouveau fichier batch commence par une lettre indiquant la phase. Par exemple T pour indiquer que le fichier vient d'être transféré. Il est suivi de la **date** de soumission au format AAAAMMJJ. Par exemple : 20160112. Celle-ci est suivie d'un **décompte** à trois chiffres qui commence à 001 et de l'**identifiant du commerçant** émis par BNP Paribas. Si vous soumettez plusieurs fichiers le même jour, vous devez définir le décompte sur 002, 003, 004, etc. L'extension du fichier doit être **.DAT**.

Le nom d'un fichier batch comprend donc quatre composants :

```
<Phase><Date><MerchantID><Counter>.dat
```

Le nom d'un fichier batch via FTP :

```
<Phase><Date><Counter><MerchantID>.dat
```

Composant	Description
Phase	T=Transféré, P= Traité (Processed en anglais)
Date	Date au format AAAAMMJJ (année, mois, jour)
Counter	Trois chiffres, décompte journalier de 001 à 999.
MerchantID	Identifiant du commerçant (MID)

Le traitement du fichier batch passe par plusieurs phases indiquées dans le nom du fichier : le fichier d'origine du commerçant débute par le caractère **T** pour « transféré ». Après traitement, le fichier batch comporte le suffixe **P (**pour processed)

Si un commerçant (ayant le MerchandID : MerchantID) soumet deux fichiers batch le même jour, ces deux fichiers sont nommés comme suit :

```
T20160112001MerchantID.dat
T20160112002MerchantID.dat
```

Remarque : après que vous ayez transmis le fichier batch, le traitement des transactions débute. Après transmission et durant le traitement, le préfixe **W** (Waiting, en attente) est ajouté au fichier. Si le fichier batch est soumis via FTP/sFTP pour traitement, la phase doit être renommée **W** après l'upload par le système du commerçant. Le traitement commence uniquement après cette étape.

```
W20160112001MerchantID.dat
W20160112002MerchantID.dat
```

Lorsque toutes les transactions de paiement ont été effectuées, la solution de paiement marque les fichiers traités, qui contiennent désormais les détails du statut de transaction, avec la lettre **P** pour « Processed » (traité) et auxquels vous pouvez accéder dans la vue par batch du back office BNP Paribas via un téléchargement :

```
P20160112001MerchantID.dat
P20160112002MerchantID.dat
```

Transfert FTP de fichiers Batch

La solution de paiement vous permet de transférer des fichiers batch automatiquement via FTP (File Transfer Protocol). Pour transférer un fichier batch via FTP/sFTP, procédez comme suit :

1. Enregistrer les données de transaction dans un fichier batch formaté
2. Chiffrer le fichier batch
3. Transférer le fichier batch
4. Changer de phase après chargement (T ® W)
5. Récupérer le fichier batch après traitement
6. Vérifier le statut des transactions

Chiffrement du fichier Batch

Pour des raisons de sécurité, les fichiers batch doivent être chiffrés avant la transmission FTP/sFTP. Pour garantir un niveau de sécurité maximum, la solution de paiement utilise un chiffrement asymétrique avec PGP (Pretty Good Privacy). Le chiffrement avec GPG (GNU Privacy Guard) est également possible. Le fichier enregistré doit toutefois avoir l'extension .PGP, sans quoi aucun traitement n'est possible.

Le haut niveau de sécurité du chiffrement PGP repose sur un processus avec deux clés : une clé privée et une clé publique. BNP Paribas vous fournit une clé publique pour le chiffrement de votre fichier batch. Le fichier batch chiffré peut ensuite être déchiffré uniquement avec la clé secrète privée de BNP Paribas.

Vous pouvez également générer une clé publique et une clé privée pour votre entreprise. La solution de paiement chiffre le fichier batch avec votre clé publique. Le fichier peut ensuite être lu uniquement avec votre clé privée secrète.

Format des fichiers Batch

Un fichier batch comprend un en-tête (Header), plusieurs enregistrements et un pied de page (footer). Chaque entrée du fichier correspond à une ligne complétée avec CRLF (touche Entrée). Les valeurs dans une ligne sont séparées par des virgules. Il s'agit du format CSV (Comma Separated Values, valeurs séparées par une virgule).

Les sections suivantes décrivent le format du fichier batch que vous transmettez à la solution de paiement et le fichier de réponse, dans lequel la solution de paiement enregistre les résultats des paiements.

Format des fichiers Batch soumis

Remarque : le fichier batch ne doit pas inclure de lignes vides au début et à la fin du fichier. Les lignes vides dans les listes sont uniquement prévues pour faciliter la lecture.

Remarque : les paramètres comme « Reason » ou « OrderDesc » peuvent ne pas contenir de virgules.

Remarque : dans les versions batch 2.x, il existe un autre champ pour <MID>. Il est donc possible pour un paramètre MasterMID de soumettre les transactions d'un SubMID

En-tête

```
Type,MerchantID,Date,Version
```

Enregistrement

```
Type,Action,<Amount>,<Currency>,<TransID>,<Data depends on Action>
```

Pied de page

```
Type,CountRecords,SumAmount
```

L'exemple suivant représente un fichier batch pour la capture de trois transactions par carte avec une valeur de 1,00 et 2,00 euros. Pour le premier paiement, le système du commerçant fournit le numéro de référence 123456, mais aucun numéro de référence n'est fourni pour le deuxième et le troisième :

```
HEAD,MerchantID,20160112,1.2


CC,Sale,100,EUR,1567890,123456,MasterCard,5490011234567890,200506,Your order from Jan. 4.

CC,Sale,100,EUR,1567891,,MasterCard,5490011234567890,200506,Your order from Jan. 4.

CC,Sale,200,EUR,10202280,,VISA,4907621234567890,200504,Your order from Jan. 4.


FOOT,3,400
```

La description de chaque champ et valeurs du jeu de données (**Enregistrements/RECORDS**) dans le fichier batch est disponible dans le chapitre correspondant du manuel sur la méthode de paiement.

Les paramètres généraux pour le transfert dans l'**en-tête** et le **pied de page** sont expliqués dans le tableau suivant :

Paramètre	Format	CND	Description
Type	a..11	M	« HEAD » pour en-tête (Header), « FOOT » pour pied de page (Footer) et, par exemple, « CC » pour carte. Le champ n'a pas à contenir 11 chiffres.
MerchantID	ans..30	M	Identifiant du commerçant (MID) fourni par BNP Paribas

Date	dttm8	M	Date de production du fichier au format AAAAMMJJ
Version	an6	M	La version batch utilisée détermine les paramètres facultatifs utilisés en addition. Les versions batch possibles dans chaque cas diffèrent selon la méthode de paiement et l'action effectuée. Vous trouverez les versions possibles dans le chapitre sur les fichiers batch de la méthode de paiement correspondante.
CountRecords	n..5	M	Nombre d'enregistrements soumis sans en-tête (header) ni pied de page (footer)
SumAmount	n..12	M	Total des montants dans l'unité de devise la plus faible, p. ex. centimes dans le cas des euros, selon le tableau des devises. Contactez l'Assistance si vous voulez capturer des montants inférieurs à 100 (unité de devise la plus faible).

Format des fichiers de reponse Batch

Lors du traitement des transactions, le gestionnaire des fichiers batch enregistre le statut de la transaction dans le fichier batch. Dans cette optique, les champs de **statut** et de **code** sont ajoutés dans les entrées de transaction dans la zone **d'enregistrement** (Record):

Enregistrement (Record)

CC,Capture,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>**,<Status>,<Code>**

Remarque : en règle générale, le retour des paramètres facultatifs dans le fichier de réponse se produit uniquement si ceux-ci étaient inclus dans le fichier soumis. En règle générale, aucune information d'envoi n'est fournie dans le fichier de réponse. Si vous avez à nouveau besoin de ces données, lisez-les à partir du paramètre de notification correspondant.

Les paramètres de réponse particuliers que le gestionnaire des fichiers batch enregistre dans la section d'enregistrement pour chaque transaction sont disponibles dans le chapitre relatif aux fichiers batch pour la méthode de paiement concernée.

Codes retours Batch

La solution de paiement prend en charge les codes d'erreur détaillés depuis la version 3.0. Il s'agit de codes hexadécimaux à huit chiffres. La structure et la signification des codes d'erreur sont décrites sur la base de l'exemple suivant :

2 105 0014

Le premier chiffre décrit le niveau de gravité de l'erreur. Toutes les valeurs supérieures à 0 indiquent un avertissement ou une erreur.

Remarque : un code d'erreur ne signifie pas nécessairement que la solution de paiement ou le système du commerçant a subi une erreur technique. La solution de paiement génère également un code d'erreur si une transaction a échoué car la banque refuse un paiement.

Les 2^{e}, 3^{e} et 4^{e} chiffres du code d'erreur décrivent la catégorie de l'erreur. Les catégories d'erreur se rapportent aux erreurs de chiffrement (001) et de format (010), et aux détails des méthodes de paiement, initiés dans le cas des cartes (100) à débit immédiats (110) ou Cash&Go (140).

Les chiffres 5 à 8 du code d'erreur fournissent une indication sur les détails de l'erreur : instructions sur les problèmes de configuration comme des identifiants de terminaux manquants (0047) et dysfonctionnements au niveau du centre informatique de la banque du porteur de carte (121), mais également des refus standard de paiements par carte en cas de cartes expirées (110) ou de messages refusés (0100).

Remarque : les transactions sans erreur, pour des raisons de compatibilité avec la version 2.1, ne sont pas spécifiées par un 8, mais **un zéro (0)**.

Vous trouverez la liste complète des codes d'erreur de la solution de paiement dans le fichier Excel.

Appels et réponses de Batch

Cette section décrit les paramètres qui doivent être transférés dans les enregistrements (Records) pour l'exécution d'un paiement par carte, et quelles informations peuvent être trouvées dans le fichier de réponse sur le statut du paiement.

La structure pour un paiement par carte dans un fichier batch à soumettre est la suivante :

HEAD,<MerchantID>,<Date>,<Version>

CC,Authorize,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>, [<CCCVC>,]<CCExpiry>,<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>]

CC,Capture,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,[<FinishAuth,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>]

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>, [<CCCVC>,]<CCExpiry>,<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>]

CC,Credit,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>[,<FinishAuth>,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>]

CC,CreditEx,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>, [<CCCVC>,]<CCExpiry>,<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>]

CC,Reverse,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>

FOOT,<CountRecords>,<SumAmount>

Exemple de versions batch :

Version 1.2:

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>,<cardholder>

Version 1.2.1:

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>

Version 1.3:

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCExpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>

Version 1.5:

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<Zone>

Le tableau suivant décrit les champs et valeurs utilisés dans le jeu de données (Record (enregistrement)) dans le fichier batch :

Paramètre	Format	CND	Description
Type	a..11	M	« HEAD » pour en-tête (header), « FOOT » pour pied de page (footer), « CC » pour carte
Action	a..20	M	Le paramètre Action définit le type de la transaction : Authorize (autorisation) Capture Sale Refund CreditEx (remboursement sans capture ; convenez de cela au préalable avec le Support BNP Paribas) Reverse (annulation) AuthSplit (capture partielle) Renewal (renouvellement d'autorisation)
Amount	n..10	M	Montant dans l'unité de devise la plus petite (p. ex. centime d'euro). Contactez l'Assistance si vous voulez capturer des montants inférieurs à 100 (unité de devise la plus faible).
Currency	a3	M	Code de devise, trois chiffres DIN / ISO 4217
TransID	ans..64	M	Identifiant de la transaction devant être unique pour chaque paiement. Notez pour certaines connexions, les différents formats fournis au sein des paramètres spécifiques.
RefNr	an12	M	Numéro de référence unique

PayID	an32	M	Identifiant de cette transaction fournie par la solution de paiement
OrderDesc	ans..127	O	Description des produits achetés, prix à l'unité, etc.
CCBrand	a..22	C	Marque de la carte. Notez bien l'orthographe ! Selon le tableau des marques de carte !
CCNr	n..16	C	Numéro de carte d'au moins 12 chiffres, numériques sans espace. Vous pouvez également transmettre un TOKEN (numéro de carte temporaire)
PCNr	n..16	O	Vous pouvez également transmettre un TOKEN (PCN) au lieu du numéro de carte réelle.
CCCVC	n..4	O	Vérification de carte : dans le cas de Visa et MasterCard, les 3 derniers chiffres sur la bande de signature de la carte. 4 chiffres dans le cas d'American Express.
CCExpiry	n6	O	Date d'expiration de la carte au format AAAAMM, p. ex. 201707.
FinishAuth	ans1	O	Version=1.4 : si vous utilisez le renouvellement d'autorisation, annulez la répétition avec la valeur Y dans le champ FinishAuth dans le cas d'une capture ou d'un remboursement. Exemple : vous capturez une livraison partielle. Le reste de la commande ne peut pas être fourni. Vous saisissez par conséquent Y dans le champ FinishAuth pour une capture partielle, afin que la solution de paiement n'autorise pas le montant restant.
RTF	a1	O	Abonnement à durée et montant **fixes** • Paiement initial : RTF=I • Echéances suivantes : RTF=R Abonnement à durée et montants **variables** • Paiement initial : RTF=E • Echéances suivantes : RTF=M

La zone d'enregistrement dans le fichier de réponse pour les transactions par batch se présente comme suit :

HEAD,<MerchantID>,<Date>,<Version>

CC,Authorize,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,]<CCExpiry>,<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>],<Status>,<Code>

CC,Capture,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>[<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>],<Status>,<Code>

CC,AuthSplit,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,FAILED,<Code>,<Description>,[<PCNr>]

CC,Renewal,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,FAILED,<Code>,<Description>,[<PCNr>]

CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,]<CCExpiry>,<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>],<Status>,<Code>

CC,Credit,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>[,<FinishAuth>,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>],<Status>,<Code>

CC,CreditEx,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,[<CCCVC>,]<CCExpiry>,<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>],<Status>,<Code>

CC,Reverse,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,<Status>,<Code>

FOOT,<CountRecords>,<SumAmount>

Le tableau suivant décrit les paramètres de réponse que le gestionnaire des fichiers batch enregistre dans la zone d'enregistrement (record) pour chaque transaction (paramètres standard non expliqués ici, comme <TransID> ou <RefNR>, et les paramètres de requête sont retournés non modifiés et correspondent à l'appel tel que spécifié auparavant) :

Paramètre	Format	CND	Description
Action	a..20	M	Le paramètre Action définit le type de la transaction : capture ou remboursement (voir ci-dessous).
PayID	an32	M	Identifiant de cette transaction fournie par la solution de paiement
Status	a..50	M	OK ou FAILED (échec)
Code	n8	M	Code d'erreur selon les codes de réponses de la solution de paiement
PCNr	n..16	C	Le TOKEN est uniquement retourné dans le cas des types de transaction Authorize ou Sale et RefundEx. Il commence par 0 et les 3 derniers chiffres correspondent à ceux du véritable numéro de carte.

In-App (Mobile SDK)

Processus d'integration d'une SDK mobile

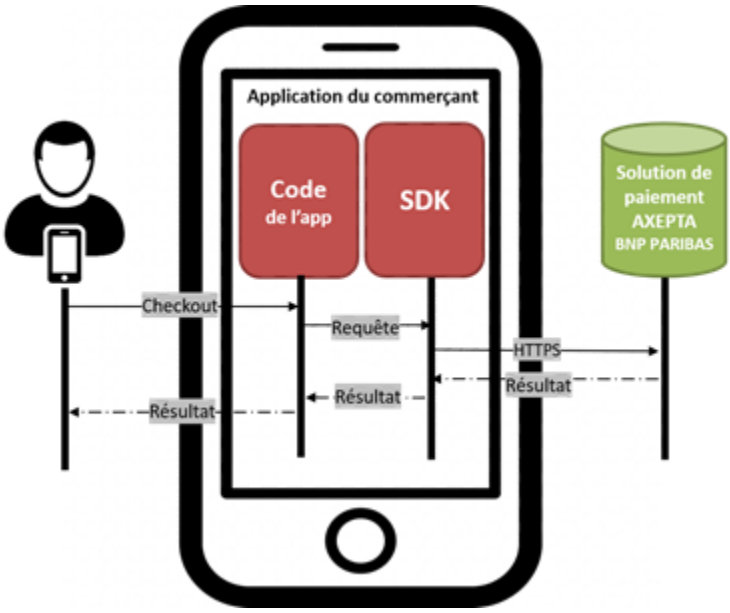
Pour le commerçant qui possède sa propre application mobile, nous fournissons un SDK mobile, c'est-à-dire un kit de développement logiciel qui contient tous les outils de programmation et les bibliothèques nécessaires à une connexion rapide et fluide de l'application du commerçant à notre solution de paiement. L'intégration des méthodes de paiement à l'application se fait via une interface sans aucun effort de développement de la part du commerçant.

Le développeur n'aura qu'à saisir les valeurs des paramètres adéquates au SDK et c'est au SDK de gérer l'authentification, la vérification, le chiffrement et le transfert des données vers la solution de paiement. C'est aussi au SDK de gérer les réponses de la solution de paiement.

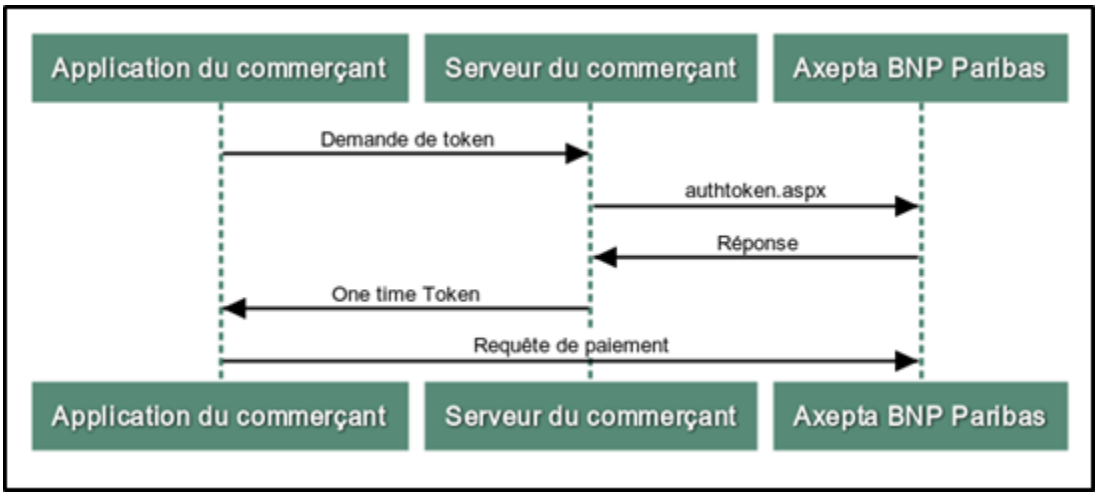
```
    /* Payment Data */
     self.paymentData = [[CMPPaymentData alloc] init];

     // Mandatory params
     self.paymentData.transID     = @"YOUR_TRANS_ID";
     self.paymentData.Amount      = @"10";
     self.paymentData.Currency    = @"EUR";
     self.paymentData.URLSuccess = @"YOUR_URL";
     self.paymentData.URLNotify   = @"YOUR_URL";
     self.paymentData.URLFailure = @"YOUR_URL";

     // some more optional params are available
}
```

Le SDK mobile est construit pour les applications natives développées en **iOS** (Version 8 au minimum) et **Android** (Version 15 - 4.0.3 au minimum) mais utilise également des « WebViews ». Ceci dépend du moyen de paiement.

Le processus de paiement est le suivant :



Cette communication est basée sur un échange de token entre les 3 acteurs principaux :



Moyens de paiement

Le SDK Mobile est valable uniquement pour les moyens de paiement suivants :

Moyen de paiement	SDK iOS	SDK Android
Cartes	✅	✅
PayPal	✅	✅
SEPA Direct Debit	✅	✅
Apple Pay	✅	
WeChat Pay	✅	✅

- Cartes

Redirection vers le formulaire de paiement par carte vers l'interface : **payssl.aspx** (pas de collecte native des données de la carte par le SDK).

- PayPal

Redirection vers la page PayPal pour se connecter : **paypal.aspx** (en utilisant le contrôleur d'affichage Safari et les onglets personnalisés Chrome).

- SEPA Direct Debit

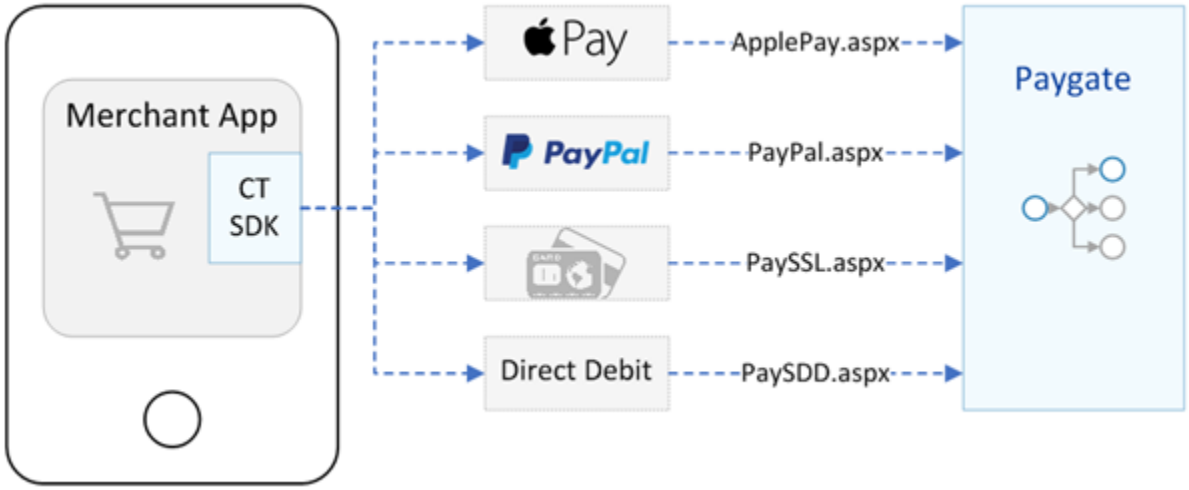
Redirection vers le formulaire de prélèvement hébergé (pas de collecte native des données IBAN par le SDK) : **paysdd.aspx**.

- Apple Pay

Apple Pay utilise une API APPLE PAY native.

- WeChat Pay

Le SDK communique avec le WeChat Pay SDK et l'application WeChat app installée dans le smartphone de l'utilisateur.



Distribution SDK

Le SDK est fourni via des injections de dépendances (Cocoa Pods / GitHub repository).

Toutes les informations nécessaires sur l'intégration du SDK sont disponibles via ce lien : https://github.com/Computop