

# Intégration du paiement par cartes



# AXEPTA

## BNP PARIBAS

### Table des matières

- Acronymes et abréviations
- Intégration du paiement par carte
  - Informations générales sur les paiement par carte
  - Le formulaire de la page de paiement et les données de cartes sont hébergés par BNP Paribas (payssl.aspx)
    - Schéma des flux
    - Exécution d'une transaction avec 3D Secure
    - Paramètres de la requête de paiement
    - Paramètres du résultat de la requête de paiement
  - Le formulaire de la page de paiement est hébergé par le commerçant et les données de carte sont hébergées par BNP Paribas (paynow.aspx)
  - Le formulaire de la page de paiement et les données de cartes sont hébergés par le commerçant (Serveur-to-Serveur)
    - Schéma des flux
    - Exécution d'une transaction avec 3D Secure via la connexion serveur-to-serveur
    - Appel de l'interface : paramètres généraux
  - Paiement par batch
- Gestion des paiements par carte
  - Capture
  - Annulation
  - Remboursement

## 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
dtm	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.

## Intégration du paiement par carte

### Informations générales sur les paiement par carte

La plateforme de paiement de BNP Paribas prend en charge les principales cartes de paiement et devises dans le monde. Les données cartes sont protégées contre tout accès non autorisé grâce au chiffrement **TLS**. Des fonctions de sécurité supplémentaires sont intégrées, comme la prévention de la fraude et la gestion des risques.

MasterCard SecureCode (UCAF), Verified by Visa (VbV), Diners ProtectBuy, JCB J/Secure et American Express SafeKey permettent de sécuriser les demandes de paiement avec une validation du porteur de la carte grâce à la technologie 3D Secure, ce qui signifie que le porteur de carte doit confirmer son identité via une fonctionnalité d'authentification.

Le traitement d'une transaction par carte peut être effectué via :

- Le formulaire de la plateforme de paiement,
- Une connexion serveur-to-serveur,
- Un transfert par batch

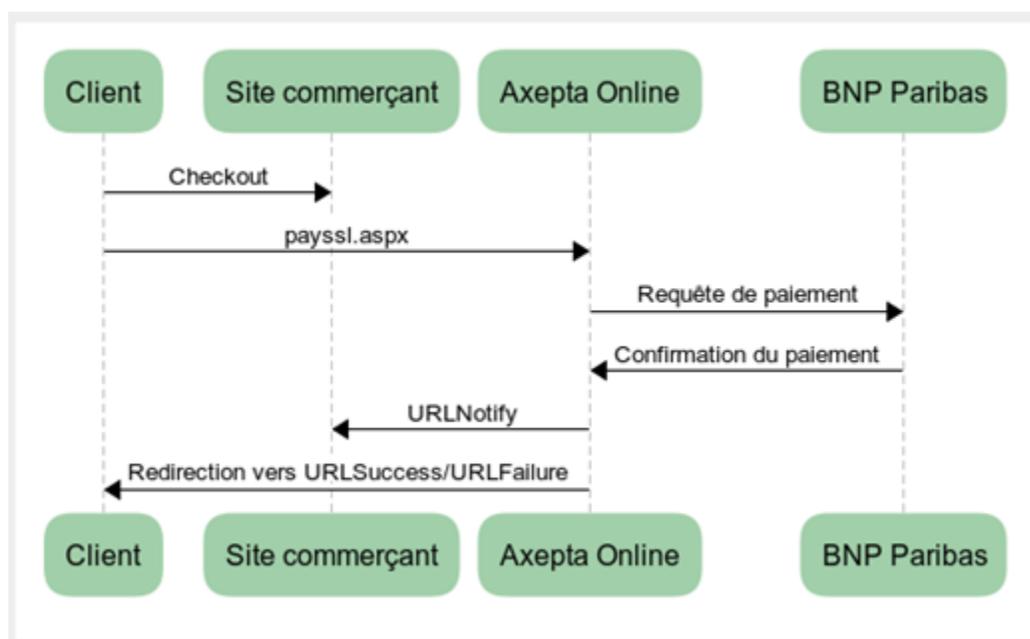
Les commerçants bénéficient du transfert de responsabilité lorsqu'ils utilisent l'authentification 3D Secure.

Sur le plan technique, le 3D Secure représente un processus d'authentification qui précède le paiement. Une fois les données de carte saisies, la plateforme de paiement vérifie l'identité du porteur de carte et le paiement n'est seulement exécuté qu'après l'authentification.

Il est essentiel de savoir si le paiement par carte est effectué via la page de paiement ou via une connexion serveur-to-serveur. Dans le premier cas, la page de paiement gère le processus d'authentification, alors que dans le cas d'une connexion serveur-to-serveur, le commerçant doit gérer l'authentification via une interface distincte.

Le formulaire de la page de paiement et les données de cartes sont hébergés par BNP Paribas (payssl.aspx)

### Schéma des flux



## Exécution d'une transaction avec 3D Secure

- Le client sélectionne le paiement par carte sur le site et saisit les informations relatives à sa carte.
- La plateforme de paiement reçoit les informations liées à la carte et vérifie, via une connexion au réseau de la carte (Visa, MasterCard, Diners, JCB, American Express) si la carte est enregistrée 3D Secure (Verified, SecureCode, Diners ProtectBuy, JCB-Card J/Secure ou SafeKey). Si la carte ne l'est pas, le paiement se fait via TLS.
- La transaction est marquée par un « flag ». Cette marque (flag) indique à la banque acquéreur que cette transaction utilise l'authentification 3DS. Cette indication est essentielle dans le cas où le porteur de la carte contesterait le paiement car elle indique à la banque le transfert de responsabilité (Liability Shift).
- La plateforme de paiement ouvre alors une fenêtre qui va permettre le client de se connecter à sa banque. Dans cette fenêtre, le client saisit le code d'accès reçu par sa banque.

**BNP PARIBAS** Identification **VISA**

**Résumé de la transaction**

Marchand : Preview Merchant  
Montant : 289,00 €  
Date : 2017-10-18T17:11:00+02:00  
N° de carte : xxxxxxxxxxxx0132  
N° de téléphone : +3362750XXXX

BNP Paribas a choisi la solution Visa Secure pour sécuriser vos achats en ligne chez les marchands référencés.

Pour vous identifier, saisissez votre code d'accès reçu par SMS:

En cas de problème, consultez l'aide en ligne en cliquant sur le lien ci-dessous.

Si le mot de passe est correct, la plateforme de paiement obtient une confirmation. Ce n'est qu'après confirmation que la plateforme de paiement débute le paiement.

**Remarque :** Veuillez noter qu'en cas de Fallback vers 3-D Secure 1.0, URLSuccess ou URLFailure est appelé avec GET. Par conséquent, vos systèmes devraient pouvoir recevoir des paramètres à la fois via GET et via POST.

## Paramètres de la requête de paiement

Pour effectuer un paiement par carte via le formulaire de la plateforme de paiement, accédez à l'URL suivante :

<https://paymentpage.axepta.bnpparibas/payssl.aspx>

Cette section décrit les paramètres à envoyer pour chaque connexion. Le second tableau décrit les paramètres de réponse qui sont identiques pour tous les paiements carte.

**Remarque :** pour des raisons de sécurité, la plateforme de paiement rejette toutes les requêtes de paiement avec des erreurs de formatage. Par conséquent, utilisez le type de donnée approprié pour chaque paramètre.

Le tableau suivant décrit les paramètres de requête de paiement chiffrés :

Paramètre	Format	CND	Description
RefNr	an12	M	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires. Notes: <ul style="list-style-type: none"><li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces, )</li><li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li></ul>
MerchantID	ans..30	M	Identifiant du commerçant désigné par BNP Paribas. Ce paramètre doit être transmis non chiffré.

<b>MsgVer</b>	ans..5	M	Valeur : 2.0   Pour <b>toutes</b> les transactions cartes (CB, Visa, Mastercard, AMEX)
<b>TransID</b>	ans..64	M	Identifiant unique de la transaction
<b>Amount</b>	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).
<b>Currency</b>	a3	M	Devise, trois chiffres selon ISO 4217
<b>MAC</b>	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
<b>URLSuccess</b>	ans..256	M	URL appelant la plateforme de paiement si le paiement a abouti. L'URL peut uniquement être appelée via le port 443. Cette URL ne doit pas contenir de paramètre: afin d'échanger les valeurs entre la plateforme de paiement et la boutique, utilisez le paramètre <b>UserData</b> (Données utilisateur).
<b>URLFailure</b>	ans..256	M	URL complète appelant la plateforme de paiement si le paiement n'a pas abouti. L'URL peut uniquement être appelée via le port 443. Cette URL ne doit pas contenir de paramètre. Afin d'échanger les valeurs entre la plateforme de paiement et la boutique, utilisez le paramètre <b>UserData</b> (Données utilisateur).
<b>Response</b>	a7	O	Réponse de statut envoyée par la plateforme de paiement à <b>URLSuccess</b> et <b>URLFailure</b> , doit être chiffrée. À cette fin, transmettez le paramètre <b>Response=encrypt</b> .
<b>URLNotify</b>	ans..256	M	URL appelée par la plateforme de paiement afin de notifier la boutique du résultat du paiement. L'URL peut uniquement être appelée via le port 443. Cette URL ne doit pas contenir de paramètre ; utilisez le paramètre <b>UserData</b> .
<b>UserData</b>	ans..1024	O	Si cela est spécifié dans la requête, la plateforme de paiement transmet le paramètre avec le résultat du paiement à la boutique
<b>Capture</b>	ans..6	O	Détermine le type et l'heure de la capture.  <b>AUTO</b> : capture immédiate après autorisation (valeur par défaut). <b>MANUAL</b> : capture effectuée par le commerçant.  <Number> : délai en heures jusqu'à la capture (nombre de 1 à 696).
<b>OrderDesc</b>	ans..768	M	Description des produits achetés, prix à l'unité, etc.
<b>ReqID</b>	ans..32	O	Pour éviter les paiements en double, saisissez une valeur alphanumérique qui identifie votre transaction et ne peut être attribuée qu'une seule fois. Si la transaction est à nouveau soumise avec le paramètre ReqID identique, la plateforme de paiement n'exécute pas le paiement et se contente de retourner le statut de la transaction d'origine. Attention : Plateforme de paiement doit afficher un statut de transaction finalisée pour la première action initiale. Les introductions avec un ReqID identique pour un statut ouvert sont traitées à intervalles réguliers.
<b>Plain</b>	ans..50	O	Valeur définie par le commerçant pour retourner certaines informations non chiffrées (p. ex. identifiant du commerçant (MID))
<b>Custom</b>	ans..1024	O	Le commerçant peut soumettre plusieurs valeurs séparées par   et qui sont retournées non chiffrées et séparées par &. Custom=session=123 id=456 devient dans la réponse Session=123&id=456
<b>expirationTime</b>	ans..19	O	Date et heure de fin du traitement de la transaction, en heure UTC. Format : AAAA-MM-jjTHH:mm:ss
<b>AccVerify</b>	a3	O	Si AccVerify=Yes, la carte sera vérifiée du côté de l'acquéreur selon la description de l'interface de l'acquéreur. Le commerçant doit soumettre uniquement ce paramètre ; le paramètre Amount est facultatif. Si Amount est utilisé, nous remplaçons le montant selon la description de l'interface de l'acquéreur. Au paiement, Amount=0 est enregistré.  Valeur autorisée : yes

Pour adapter la mise en page de la page SSL de votre boutique, vous pouvez utiliser les paramètres non chiffrés suivants :

Paramètre	Format	CND	Description
<b>Template</b>	ans..20	O	Nom du fichier XSLT avec votre propre mise en page pour le formulaire de paiement. Si vous voulez utiliser le modèle BNP Paribas repensé et avec rétrocompatibilité, transférez le nom de modèle « ct_compatible ». Si vous voulez utiliser le modèle BNP Paribas réactif ( <b>responsive</b> ) pour les périphériques mobiles, transférez le nom de modèle « ct_responsive ».
<b>Language</b>	a2 (enum)	O	Code de langue : <de> allemand, <en> anglais, <fr> français, <it> italien, <n> néerlandais, <pt> portugais, <es> espagnol  La langue par défaut est le français.
<b>URLBack</b>	ans..256	O	URL pour le bouton « Annuler »
<b>CCSelect</b>	a..16	O	Détermine le type de carte présélectionnée dans le formulaire
<b>CustomField [n]</b>	Ans..50	O	Champs pouvant être utilisés par le commerçant. Nous proposons actuellement 9 champs. De « CustomField1 » à « CustomField9 »

## Paramètres du résultat de la requête de paiement

Le tableau suivant décrit les paramètres du résultat transmis par la plateforme de paiement à **URLNotify**, **URLSuccess** ou **URLFailure**. Si vous avez spécifié le paramètre **Response=encrypt**, les paramètres suivants sont envoyés chiffrés avec la méthode Blowfish à votre système :

Paramètre	Format	CND	Description
<b>RefNr</b>	an12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces)</li> <li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li> <li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li> </ul>
<b>MID</b>	ans..30	M	Identifiant du commerçant (MerchantID) attribué par BNP Paribas.
<b>PayID</b>	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement ; p. ex. pour référencement dans les fichiers batch
<b>XID</b>	an32	M	Identifiant pour toutes les transactions uniques (autorisation, capture, remboursement) pour un paiement attribué par la plateforme de paiement
<b>TransID</b>	ans..64	M	Numéro de transaction du commerçant
<b>Status</b>	a..50	M	OK / AUTHORIZED (URLSuccess) / FAILED (URLFailure)
<b>Description</b>	ans..1024	M	Détails supplémentaires dans le cas où le paiement est rejeté. N'utilisez pas la <b>Description</b> , mais le paramètre <b>Code</b> pour l'analyse du statut de transaction !
<b>Code</b>	n8	M	Code erreur de réponses de la plateforme de paiement (voir fichier Excel des codes erreur)
<b>MAC</b>	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
<b>UserData</b>	ans..1024	O	Si cela est spécifié dans la requête, la plateforme de paiement transmet le paramètre avec le résultat du paiement à la boutique
<b>PCNr</b>	n16	O	TOKEN (Pseudo Card Number, numéro de carte temporaire) : numéro aléatoire généré par la plateforme de paiement qui représente un numéro de carte authentique. Le TOKEN (PCN) commence par 0, et les 3 derniers chiffres correspondent à ceux du véritable numéro de carte. Vous pouvez utiliser le PCN comme un numéro de carte authentique pour une autorisation, une capture et un remboursement.
<b>CCBrand</b>	a..22	OC	Désignation de la marque de carte
<b>CCEpiry</b>	n6	OC	En combinaison avec PCNr : date d'expiration de la carte au format AAAAMM (201706).
<b>maskedpan</b>	an..19	OC	Numéro de carte masqué 6X4
<b>CAVV</b>	ans..40	OC	Dans le cas de 3D Secure avec hébergement d'authentification (requête 3D sans autorisation uniquement) : valeur de validation d'authentification de porteur de carte : contient la signature numérique pour l'authentification avec l'ACS de la banque émettrice de la carte.
<b>ECI</b>	n2	OC	Pour 3D Secure : l'indicateur d'e-commerce ACS : définit le niveau de sécurité d'un paiement par carte via les différents canaux de communication : MOTO, SSL, Verified by Visa, etc.
<b>DDD</b>	a1	C	Pour l'hébergement d'authentification 3D Secure :  Y - entièrement authentifié (authentification complète effectuée)  N - not enrolled (vérifié, mais l'émetteur ne participe pas)  U - non éligible (erreur technique)  A - attempt (la carte ne participe pas)  B - bypass (contournement, uniquement pour CardinalCommerce)
<b>Type</b>	ans..20	C	Pour 3D Secure uniquement, en réponse à URLNotify : abréviation du type de paiement, (exemple : SSL)
<b>Plain</b>	ans..50	O	Une valeur définie par le commerçant pour retourner certaines informations non chiffrées (p. ex. identifiant du commerçant)
<b>Custom</b>	ans..1024	O	Le commerçant peut soumettre plusieurs valeurs séparées par   et qui sont retournées non chiffrées et séparées par &. Custom=session=123 id=456 devient dans la réponse Session=123&id=456
<b>CustomField [n]</b>	ans..50	O	Champ pouvant être utilisé individuellement par le commerçant. Actuellement, 9 champs de CustomField1 à CustomField9 sont pris en charge.
<b>CodeExt</b>	an2	O	Code d'erreur de CAPN.
<b>Approvalcode</b>	an..6	O	Code d'autorisation de la transaction
<b>TerminalID</b>	n..7	O	TerminalID utilisé pour le processing

<b>VUNr</b>	n..7	O	Numéro de contact d'acquisition
<a href="#">schemeReferencelD</a>	ans..64	O	Générée par la banque du porteur ou le réseau Cette donnée sera stockée par le marchand et utilisée pour chaîner les transactions récurrentes à la 1ère transaction d'un abonnement (cas du paiement récurrent seulement) <a href="#">Paiement récurrent carte (Abonnement)</a>

## Le formulaire de la page de paiement est hébergé par le commerçant et les données de carte sont hébergées par BNP Paribas (paynow.aspx)

Même processus 3DS que pour payssl.aspx

Un Silent-order post associe les avantages des formulaires de la plateforme de paiement et de la connexion serveur-to-serveur : contrairement au formulaire de la plateforme de paiement, où le formulaire est chargé depuis le serveur de la plateforme de paiement via l'appel de **payssl.aspx**, le Silent order post doit être fourni par le système du commerçant. Le formulaire utilise les mêmes paramètres que ceux décrits ci-dessous.

Contrairement au formulaire de la plateforme de paiement, les paramètres ne sont pas transférés en tant que paramètres d'URL comme c'est le cas lors de l'appel payssl.aspx, mais en tant que paramètres de saisie du formulaire.

Payssl	Paynow
payssl.aspx?MerchantID=[mid]&Len=[len]&Data=[data]	<pre>&lt;form action=paynow.aspx&gt; &lt;input type="hidden" name="MerchantID" value=[mid]&gt; &lt;input type="hidden" name="Len" value=[len]&gt; &lt;input type="hidden" name="Data" value=[data]&gt; : &lt;/form&gt;</pre>

Les données de carte doivent être transmises à paynow.aspx avec les paramètres suivants :

Paramètre	Format	CND	Description
<b>CCNr</b>	n..16	M	Numéro de carte d'au moins 12 chiffres, numérique sans espace
<b>CCCVC</b>	n3	O	Numéro de vérification de carte : les trois derniers chiffres sur la bande de signature de la carte
<b>CCEpiry</b>	n6	M	Date d'expiration de la carte au format AAAAMM, p. ex. 201807.
<b>CCBrand</b>	a..22	M	Désignation de la marque de carte. Notez bien l'orthographe ! Selon le tableau des marques de carte !

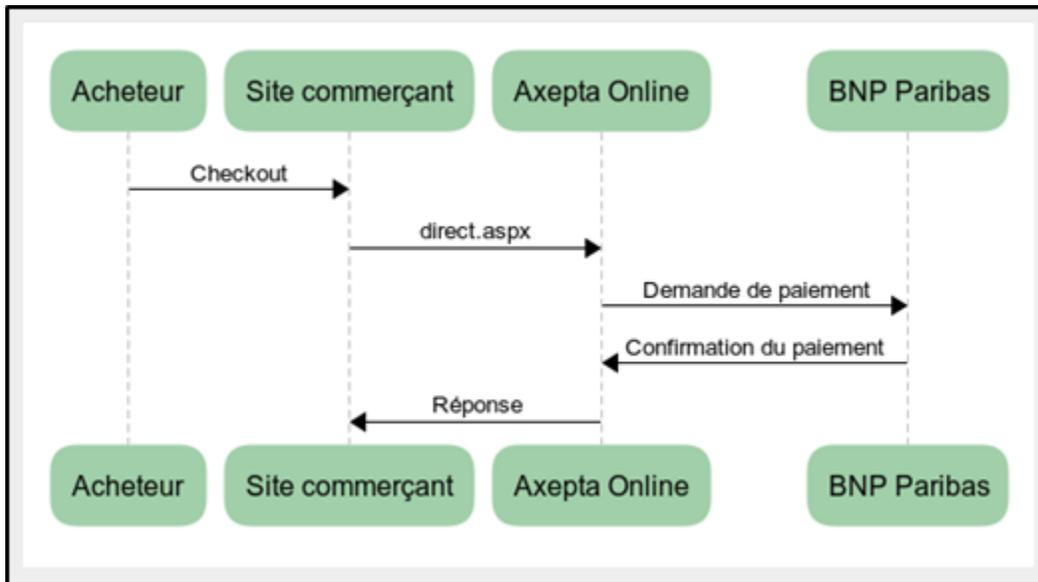
Une fois que le client a saisi les données de sa carte, les données de paiement sont transférées à la page Silent order post où le paiement est exécuté via 3D Secure. Les détails du formulaire doivent être directement transférés à la page Silent order post, mais ne doivent pas être transmis au système du commerçant. De plus, il se peut qu'aucune donnée PCI ne soit transmise à la page Silent order post en tant que paramètres de saisie supplémentaires.

**Remarque :** les nouvelles tentatives automatiques au niveau de la plateforme de paiement doivent être désactivées lors de l'utilisation de Paynow.aspx. En effet, lors d'une nouvelle tentative, la plateforme de paiement ne peut pas rediriger le client vers le formulaire de saisie de la boutique précédemment utilisé. Contactez le Support BNP Paribas pour désactiver les nouvelles tentatives.

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

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

### Schéma des flux



## Exécution d'une transaction avec 3D Secure via la connexion serveur-to-serveur

Pour procéder à l'authentification, la plateforme de paiement connecte le porteur de carte à sa banque, qui confirme son identité. Un paiement exécuté avec Verified by Visa, MasterCard SecureCode, Diners ProtectBuy, JCB-Card J/Secure ou American Express SafeKey se fait en deux étapes : authentification et paiement.

Dans les étapes suivantes, la plateforme de paiement répond différemment dans deux situations :

- **Cas 1: Authentification 3D Secure via une page affichée en pop-up**

Si la carte est enregistrée pour Verified, SecureCode, ProtectBuy, J/Secure ou SafeKey, la plateforme de paiement retourne une page HTML affichée en pop-up (fenêtre superposée). Cette page HTML (qui contient une fonction en Javascript appelée « Initiate3DSec() ») effectue la connexion avec la banque du porteur de la carte et permet de faire la correspondance entre le code entré par le porteur (client de la boutique) et le code envoyé par la banque.

**Remarque :** l'utilisation d'une fenêtre séparée peut entraîner des problèmes avec les bloqueurs de fenêtres contextuelles (pop-up) dans le navigateur du client. Par conséquent, le cas 2 décrit une alternative sous la forme d'une variante iFrame.

L'exemple suivant présente une page dans laquelle le code HTML est intégré :

```
<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=unicode">
  <SCRIPT language="javascript">
<!--
<Response excerpt from request: HTML with JavaScript>
  //-->
  </script>
  </HEAD>");
  <BODY onload="javascript:Initiate3DSec();">
<table><tr>
<td align="center"><font face="Verdana" size="-1"><b>Please identify yourself with 3D Secure!</b></font></td>
</tr></table>");
</BODY>
</HTML>
```

**Remarque** : vous pouvez aussi utiliser ce code si vous voulez uniquement vérifier l'identité du porteur de la carte sans procéder à un paiement par carte. Notre équipe support peut paramétrer votre compte de façon à ce que la plateforme de paiement puisse procéder à l'authentification avec Verified, SecureCode, ProtectBuy, J/Secure ou SafeKey sans faire de paiement (**Authentication hosting**).

Lorsque le client a été authentifié grâce à sa banque, le serveur de contrôle d'accès (ACS, Access Control Server) de la banque appelle l' url TermURL de la boutique. Dans le cas de cette requête, l'ACS transfère les paramètres suivants via GET (QueryString) à l'url TermURL de la boutique : MID, PayID et TransID. Le paramètre PAREs est transféré via POST.

**Remarque** : le paramètre PAREs doit être URL-encoded, mais non chiffré avec la méthode Blowfish, car le contenu peut inclure des caractères spéciaux.

Le paramètre doit être transféré dans son intégralité via la méthode POST à l'URL suivante :

<https://paymentpage.axepta.bnpparibas/direct3d.aspx>

**Remarque** : si vous transférez les paramètres PAREs et MID, utilisez les paramètres MerchantID (identifiant du commerçant) et PAREs pour la page direct3d.aspx.

#### • Cas 2: Authentification 3D Secure via une page affichée en iFrame

Une alternative au pop-up, le commerçant peut choisir l'iFrame comme méthode d'affichage de la page d'authentification 3DS. Le porteur de carte peut effectuer l'authentification auprès de sa banque sur la page où il se trouve via une autre interface affichée en iFrame ; cela évite les difficultés rencontrées avec les bloqueurs de fenêtres contextuelles (pop-up) dans le navigateur du client.

Si la carte est enregistrée sur le serveur (Directory Server), la plateforme de paiement renvoie les paramètres suivants via la connexion socket.

Paramètre	Format	CND	Description
ACSURL	ans..	C	Uniquement dans le cas des cartes enregistrées : URL du serveur de contrôle d'accès de l'émetteur de carte avec paramètres de requête joints (sans encodage URL). Il est possible d'utiliser l'esperluette et le point d'interrogation du serveur ACS comme valeurs dans l'URL ; tout caractère précédant le paramètre PAREq fait partie d'ACSURL.
PaReq	ans..	M	Requête d'authentification du payeur (URL-encoded)
MD		M	Les données du commerçant sont une valeur vide, qui doit être transférée pour des raisons de compatibilité
TermURL	ans..	M	Adresse de retour de la boutique. La plateforme de paiement ajoute les paramètres PayID, TransID et MID comme paramètres de demande au TermURL initial séparés par un point d'interrogation.

#### Exemple de traitement correct d'ACSURL et de TermURL :

acsurl=a?b=c&d=e&pareq=f&termurl=g?PayID=h&TransID=i&MID=j

ACSURL: a?b=c&d=e

TermURL: g?PayID=h&TransID=i&MID=j

**Remarque** : dans ce processus, les données doivent parfois être transférées directement depuis le réseau de la banque. Par conséquent, le paramètre ACSURL n'est pas URL-encoded, bien que la plateforme de paiement utilise d'autres données URL-encoded.

Ces paramètres doivent être inclus en tant que champs MASQUÉS dans une page HTML qui poste elle-même vers l'URL ACS. L'exemple suivant présente cette page HTML, dans laquelle les paramètres de retour sont intégrés :

```

<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=unicode">
<A content="MSHTML 6.00.2800.1106" name=GENERATOR>
</HEAD>
<BODY onload="sendpareq.submit();">
<FORM action="[ACSURL]" method="POST" name="sendpareq">
<input type="hidden" name="MD" value="">
<input type="hidden" name="PaReq" value="[PaReq]">
<input type="hidden" name="TermUrl" value="[TermUrl]">
</FORM>
</BODY>
</HTML>

```

**Remarque :** vous pouvez aussi utiliser ce code si vous voulez uniquement vérifier l'identité du porteur de carte sans procéder immédiatement à un paiement par carte (hébergement d'authentification). Le Support BNP Paribas peut configurer votre paiement, afin que la plateforme de paiement puisse appliquer le Verified by Visa ou le SecureCode sans paiement.

Lorsque le client a été authentifié grâce à sa banque, le serveur de contrôle d'accès (ACS, Access Control Server) de la banque appelle l'url TermURL de la boutique. Dans le cas de cette requête, l'ACS transfère les paramètres suivants via GET (QueryString) via l'url TermURL de la boutique : MID, PayID et TransID (sans chiffrement). Le paramètre PAREs est transféré sans chiffrement via POST.

**Remarque :** le paramètre PAREs doit être encodé au format URL, mais non chiffré avec la méthode Blowfish, car le contenu peut inclure des caractères spéciaux.

Le paramètre doit être transféré dans son intégralité via POST à l'URL suivante :

<https://paymentpage.axepta.bnpparibas/direct3d.aspx>

**Remarque :** si vous transférez les paramètres ACS, PAREs et MID, utilisez l'identifiant du commerçant et PAREs pour la page direct3d.aspx.

## Appel de l'interface : paramètres généraux

**Remarque :** pour les paiements par carte avec 3D Secure, prenez connaissance des différents cas expliqués dans le chapitre précédent. Si la carte est enregistrée pour Verified, SecureCode ou SafeKey, la phase suivante est divisée en deux étapes : authentification et paiement. Toutefois, cela commence toujours de la même façon via l'interface **direct.aspx**. La première réponse correspond à la réception du code JavaScript ou d'autres paramètres afin de procéder à un second appel de l'interface **direct3d.aspx**. Ce n'est qu'après que vous recevez le paramètre répertorié en tant que réponse.

**i** La carte doit être encore valide au moment de la saisie / du remboursement. BNP Paribas accepte donc les cartes lorsqu'elles sont valables au moins 1 semaine avant leurs expirations (par ex. CC expire : 2020-03 autorisations possibles jusqu'au 2020-03-24, 23:59:59).

Pour procéder à un paiement par carte TLS via une connexion serveur-to-serveur, appelez l'URL suivante :

<https://paymentpage.axepta.bnpparibas/direct.aspx>

**Remarque :** pour des raisons de sécurité, la plateforme de paiement rejette toutes les requêtes de paiement avec des erreurs de formatage. Par conséquent, utilisez le type de donnée approprié pour chaque paramètre.

Le tableau suivant décrit les paramètres de requête de paiement chiffrés :

Paramètre	Format	CND	Description
-----------	--------	-----	-------------

<b>RefNr</b>	an12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"><li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces)</li><li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li><li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li></ul>
<b>MerchantID</b>	ans..30	M	Identifiant du commerçant (MID) attribué par BNP Paribas. Ce paramètre doit être transmis non chiffré.
<b>MsgVer</b>	ans..5	M	Version du message  Valeur acceptée : 2.0
<b>TransID</b>	ans..64	M	Identifiant de la transaction devant être unique pour chaque paiement
<b>Amount</b>	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).
<b>Amount3D</b>	n..10	OC	Uniquement pour 3D Secure : montant pour l'authentification avec Verified, SecureCode et SafeKey si le montant est différent. Par exemple : le client confirme le prix d'un vol de 120 euros avec Verified, mais l'agent de voyage capture uniquement les frais de réservation de 20 euros : <b>Amount3D=12 000; Amount=2 000</b> . 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).
<b>Currency</b>	a3	M	Devise, trois chiffres DIN / ISO 4217
<b>CCNr</b>	n..19	M	Numéro de carte d'au moins 12 chiffres, numérique sans espace. Vous pouvez également transmettre un numéro PCN. (pseudo card number).
<b>CCCVC</b>	n..4	O	Numéro de vérification de carte (CVV) : pour Visa et MasterCard, les 3 derniers chiffres sur la bande de signature de la carte. Pour American Express, les 4 derniers chiffres.
<b>CCEpiry</b>	n6	M	En combinaison avec TOKEN : date d'expiration de la carte au format AAAAMM (201706).
<b>CCBrand</b>	a..22	M	Désignation de la marque de carte.  Notez bien l'orthographe ! Selon le tableau des marques de carte !
<b>Capture</b>	ans..6	O	Détermine le type et l'heure de la capture. <b>AUTO</b> : capture immédiate après autorisation (valeur par défaut). <b>MANUAL</b> : capture effectuée par le commerçant. <b>&lt;Number&gt;</b> : délai en heures jusqu'à la capture (nombre entier : 1 à 696).
<b>OrderDesc</b>	ans..768	M	Description des produits achetés, prix à l'unité, etc.
<b>TermURL</b>	ans..256	C	Uniquement pour 3D Secure. URL de la boutique sélectionnée par le serveur ACS (Access Control Server) de la banque du porteur de carte pour la transmission du résultat de l'authentification. La banque transfère les paramètres suivants : PayID, TransID et MerchantID via GET et le paramètre PAResponse via POST à TermURL.
<b>UserAgent</b>	ans..128	C	Uniquement pour 3D Secure. Type de navigateur de l'utilisateur appelant la page. Par exemple : IE Mozilla/4.0 (compatible ; MSIE 6.0 ; Windows NT 5.0 ; NET CLR 1.0.3705)
<b>HTTPAccept</b>	ans..128	C	Uniquement pour 3D Secure : types MIME que les clients du commerçant acceptent. P. ex. image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
<b>MAC</b>	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
<b>ReqID</b>	ans..32	O	Pour éviter les paiements en double, saisissez une valeur alphanumérique qui identifie votre transaction et ne peut être attribuée qu'une seule fois. Si la transaction est à nouveau soumise avec le paramètre ReqID identique, la plateforme de paiement n'exécute pas le paiement et se contente de retourner le statut de la transaction d'origine. Attention : Plateforme de paiement doit afficher un statut de transaction finalisée pour la première action initiale. Les introductions avec un ReqID identique pour un statut ouvert sont traitées à intervalles réguliers.
<b>AccVerify</b>	a3	O	Si AccVerify=Yes, la carte sera vérifiée du côté de l'acquéreur. alors Le commerçant doit soumettre le paramètre AccVerify (obligatoire) et peut utiliser le paramètre Amount (facultatif) pour ajouter un montant . La valeur par défaut du montant (amount) est 0

Le tableau suivant fournit les paramètres avec lesquels la plateforme de paiement répond :

Paramètre	Format	CND	Description
<b>MID</b>	ans..30	M	Identifiant du commerçant
<b>PayID</b>	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement ; p. ex. pour référencement dans les fichiers batch
<b>XID</b>	an32	M	Identifiant pour toutes les transactions uniques (autorisation, capture, remboursement) pour un paiement attribué par la plateforme de paiement
<b>TransID</b>	ans..64	M	Numéro de transaction du commerçant
<b>Status</b>	a..50	M	OK ou AUTHORIZED (URLSuccess) et FAILED (URLFailure)

<b>Description</b>	ans..1024	M	Détails complémentaires dans le cas où le paiement est rejeté. N'utilisez pas la <b>Description</b> , mais le paramètre <b>Code</b> pour l'analyse du statut de transaction !
<b>Code</b>	n8	M	Code d'erreur selon les codes de réponses de la plateforme de paiement
<b>PCNr</b>	n16	O	TOKEN (Pseudo Card Number) : numéro aléatoire généré par la plateforme de paiement qui représente un numéro de carte. Le TOKEN (PCN) commence par 0, et les 3 derniers chiffres correspondent à ceux du véritable numéro de carte. Vous pouvez utiliser le PCN comme un numéro de carte pour l'autorisation, la capture et les remboursements.
<b>CCEpiry</b>	n6	OC	En combinaison avec TOKEN : date d'expiration de la carte au format AAAAMM (201706).
<b>CCBrand</b>	a..22	OC	En combinaison avec PCNr : Désignation de la marque de carte Notez bien l'orthographe ! Selon le tableau des marques de carte !
<b>maskedpan</b>	an..19	OC	Numéro de carte masqué 6X4
<b>CAVV</b>	ans..40	OC	Dans le cas de 3D Secure avec hébergement d'authentification (uniquement requête 3D sans autorisation) : valeur de validation d'authentification de porteur de carte : contient la signature numérique pour l'authentification avec l'ACS de la banque émettrice de la carte.
<b>ECI</b>	n2	OC	Pour 3D Secure : indicateur d'e-commerce ACS : définit le niveau de sécurité d'un paiement par carte via les différents canaux de communication : MOTO, SSL, Verified by Visa, etc.
<b>DDD</b>	a1	C	Pour l'hébergement d'authentification 3D Secure : Y - entièrement authentifié (authentification complète effectuée) N - non abonné (vérifié, mais l'émetteur ne participe pas) U - non éligible (erreur technique) A - tentative (la carte ne participe pas) B - contournement (contournement, uniquement pour CardinalCommerce)
<b>ACSXID</b>	ans..40	O	Uniquement pour les cas 2 et 3 (avec et sans fenêtre séparée : pages 31 et 32 de ce guide) avec hébergement d'authentification : identifiant de transaction. Le paramètre ACSXID est transféré avec l'autorisation à l'acquéreur

#### Paramètres supplémentaires pour la connexion AMEX CAPN

Outre les paramètres généraux décrits ci-dessus pour la connexion de carte, AMEX exige les paramètres supplémentaires suivants :

Paramètre	Format	CND	Description
<b>RefNr</b>	an12	M	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, pas de caractères spéciaux comme les espaces)</li> <li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li> </ul>
<b>AmountAuth</b>	n..10	M	Carte prépayée : montant actuellement autorisé dans la plus petite unité de la devise
<b>ContractID</b>	n..8	O	Autre référence pouvant être utilisée pour récupérer la combinaison TerminalID/numéro de cocontractant
<b>Coordonnées/vérification d'adresse (AVS)</b>			
<b>FirstName</b>	ans..15	O	Prénom du client
<b>LastName</b>	ans..30	O	Nom du client
<b>AddrStreet</b>	ans..20	O	Rue et numéro, par ex. 18850-N-56-ST-#301
<b>AddrZip</b>	n..9	O	Code postal
<b>eMail</b>	ans..60	O	Adresse e-mail du client
<b>Phone</b>	n..10	O	Numéro de téléphone du client : pour les pays qui n'utilisent pas ce système, veuillez envoyer les 10 derniers chiffres
<b>sdFirstName</b>	ans..15	O	Prénom dans l'adresse de livraison
<b>sdLastName</b>	ans..30	O	Nom dans l'adresse de livraison
<b>sdStreet</b>	ans..50	O	Rue et numéro dans l'adresse de livraison, par ex. 4102-N-289-ST-#301
<b>sdZip</b>	n..9	O	Code postal dans l'adresse de livraison

<b>sdCountryCode</b>	n3	O	Code de pays dans l'adresse de livraison conformément à la norme ISO-3166-1, codes numériques (3 chiffres)
<b>sdPhone</b>	ans..10	O	Numéro de téléphone dans l'adresse de livraison : pour les pays qui n'utilisent pas ce système, veuillez envoyer les 10 derniers chiffres

Le tableau ci-dessous contient les paramètres utilisés par la plate-forme de paiement dans la réponse :

Paramètre	Format	CND	Description
<b>CodeExt</b>	n..10	O	Code d'erreur de CAPN
<b>ApprovalCode</b>	n..6	O	Code d'autorisation de la transaction
<b>TransactionID</b>	ans..48	O	ID de transaction de CAPN
<b>AmountAuth</b>	n..10	M	Montant autorisé dans la plus petite unité de la devise. Pour les cartes prépayées, ce montant peut être inférieur au montant initialement demandé.
<b>Match</b>	a1	O	Résultat total de la vérification des adresses (American Express via CAPN) : pour les valeurs possibles, voir le manuel Paramètres de correspondance.
<b>cvcmatch</b>	a1	C	Résultat de la vérification CVC. Valeurs possibles : M = correspondance, N = pas de correspondance, U = émetteur pas en mesure de traiter la demande

## Paielement par batch

Cette section présente les paramètres qui doivent être transmis dans les enregistrements du fichier Batch (Record) pour l'exécution d'un paiement par carte, ainsi que les informations pouvant être contenues dans le fichier de réponse concernant l'état du paiement.

La structure devant être utilisée pour un paiement par carte au sein d'un fichier Batch est comme suit :

```

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

CC,Authorize,<Amount>,<Currency>,<TransID>,(<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEXpiry>,<OrderDesc>[,<textfield1>,<textfield2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>]

CC,Capture,<Amount>,<Currency>,<TransID>,(<refnr>,<PayID>,[<FinishAuth>,<textfield1>,<textfield2>,<approvalcode>]

CC,Sale,<Amount>,<Currency>,<TransID>,(<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEXpiry>,<OrderDesc>[,<textfield1>,<textfield2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>]

CC,Credit,<Amount>,<Currency>,<TransID>,(<refnr>,<PayID>[,<FinishAuth>,<textfield1>,<textfield2>]

CC,CreditEx,<Amount>,<Currency>,<TransID>,(<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEXpiry>,<OrderDesc>[,<textfield1>,<textfield2>]

CC,Reverse,<Amount>,<Currency>,<TransID>,(<refnr>,<PayID>

FOOT,<CountRecords>,<SumAmount>

```

Exemple de différentes 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>,<textfield1>,<textfield2>,<RTF>,<cardholder>,<transactionID>,<schemeReferenceID>

Version 1.2.1

CC,Sale,<Amount>,<Currency>,<TransID>,(<refnr>,<CCBrand>,<CCNr|PCNr>,<CCEXpiry>,<OrderDesc>,<textfield1>,<textfield2>,<RTF>,<approvalcode>,<cardholder>,<transactionID>,<schemeReferenceID>

Version 1.3 :

CC,Sale,<Amount>,<Currency>,<TransID>,(<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEXpiry>,<OrderDesc>,<textfield1>,<textfield2>,<transactionID>,<schemeReferenceID>

Version 1.5 :

CC,Sale,<Amount>,<Currency>,<TransID>,(<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEXpiry>,<OrderDesc>,<Zone>

```

Le tableau ci-dessous présente les différents champs et valeurs utilisés dans l'enregistrement (record) au sein du fichier batch :

Paramètre	Format	CND	Description
RefNr	an12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, pas de caractères spéciaux)</li> <li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li> </ul>
Type	a..11	M	HEAD pour en-tête (header), FOOT pour pied de page (footer) et CC pour carte
Action	a..20	M	Le paramètre Action définit le type de transaction :  Autorize (autorisation)  Capture  Sale  Remboursement  CreditEx (remboursement sans capture préalable; veuillez confirmer cela avec le service Support)  Reverse (annulation)
Amount	n..10	M	Montant indiqué dans la plus petite unité de la devise (par ex. les centimes pour l'euro).  Veuillez contacter notre service d'assistance si vous souhaitez capturer des montants inférieurs à 100 (plus petite unité de la devise).
Currency	a3	M	Code pour la devise, trois caractères DIN / ISO 4217
TransID	an..64	M	ID de la transaction qui doit être unique pour chaque paiement
PayID	an32	M	ID pour cette transaction attribuée par la plateforme de paiement
OrderDesc	ans..127	O	Description des marchandises achetées, des prix unitaires etc.
CCBrand	a..22	C	Réseau auquel appartient la carte de paiement.  Veuillez respecter l'orthographe, Voir le tableau des réseaux des cartes (dans le guide d'intégration de la page de paiement).
CCNr	n..16	C	Numéro de la carte, minimum 12 chiffres sans espaces. Alternativement, vous pouvez transmettre un pseudo-numéro de carte (PCN)
PCNr	n..16	O	Optionnel, vous pouvez également transmettre un pseudo-numéro de carte (PCN) au lieu du vrai numéro de la carte.
CCCVC	n..4	O	Code de vérification de la carte en version 1.3 : les 3 derniers chiffres sur le champ de signature de la carte s'il s'agit de Visa et de MasterCard. 4 chiffres s'il s'agit d'American Express.
CCEpiry	n6	O	Date d'expiration de la carte au format AAAAMM, par 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 crédit. Exemple : vous prélevez le montant d'une livraison partielle. Le reste de la commande ne peut pas être livré. Vous saisissez donc Y dans le champ FinishAuth pour la capture partielle afin que la plateforme de paiement n'autorise pas le montant restant.
RTF	a1	O	Abonnement à durée et montant <b>fixes</b> <ul style="list-style-type: none"> <li>• Paiement initial : RTF=I</li> <li>• Echéances suivantes : RTF=R</li> </ul> Abonnement à durée et montants <b>variables</b> <ul style="list-style-type: none"> <li>• Paiement initial : RTF=E</li> <li>• Echéances suivantes : RTF=M</li> </ul>

La zone d'enregistrement (Record) dans le fichier de réponse pour batch transaction :

```

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

CC,Authorize,<Amount>,<Currency>,<TransID>,<refnr>,<PayID>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,<CCEpiry>,<OrderDesc>[,<textfield1>,<textfield2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>],<Status>,<Code>

CC,Capture,<Amount>,<Currency>,<TransID>,<refnr>,<PayID>[,<textfield1>,<textfield2>,<approvalcode>],<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>,<CCEpiry>,<OrderDesc>[,<textfield1>,<textfield2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>],<Status>,<Code>

CC,Credit,<Amount>,<Currency>,<TransID>,<refnr>,<PayID>[,<FinishAuth>,<textfield1>,<textfield2>],<Status>,<Code>

CC,CreditEx,<Amount>,<Currency>,<TransID>,<refnr>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,<CCEpiry>,<OrderDesc>[,<textfield1>,<textfield2>],<Status>,<Code>

CC,Reverse,<Amount>,<Currency>,<TransID>,<refnr>,<PayID>,<Status>,<Code>

FOOT,<CountRecords>,<SumAmount>

```

Exemple de différentes versions batch :

```

Version 1.2:

CC,Sale,<Amount>,<Currency>,<TransID>,<refnr>,<CCBrand>,<CCNr|PCNr>,<CCEpiry>,<OrderDesc>,<Status>,<Code>

CC,Sale,<Amount>,<Currency>,<TransID>,<refnr>,<CCBrand>,<CCNr|PCNr>,<CCEpiry>,<OrderDesc>,<textfield1>,<textfield2>,<RTF>,<cardholder>,<transactionID>,<schemeReferenceID>,<Status>,<Code>

Version 1.21:

CC,Sale,<Amount>,<Currency>,<TransID>,<refnr>,<CCBrand>,<CCNr|PCNr>,<CCEpiry>,<OrderDesc>,<textfield1>,<textfield2>,<RTF>,<approvalcode>,<cardholder>,<transactionID>,<schemeReferenceID>,<Status>,<Code>

Version 1.3:

CC,Sale,<Amount>,<Currency>,<TransID>,<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>,<textfield1>,<textfield2>,<transactionID>,<schemeReferenceID>,<Status>,<Code>

Version 1.5:

CC,Sale,<Amount>,<Currency>,<TransID>,<refnr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>,<Zone>,<Status>,<Code>

```

Le tableau ci-dessous indique les paramètres de réponse que le gestionnaire de fichier Batch (Batch Manager) sauvegarde dans la zone d'enregistrement (Record) pour chaque transaction (les paramètres par défaut non détaillés ici tels que <TransID> ou <refnr>, ainsi que les paramètres de requête sont retournés inchangés et correspondent à l'appel tel que spécifié plus haut) :

Paramètre	Format	CND	Description
Action	a..20	M	Le paramètre Action définit le type de transaction comme pour Capture ou Credit – voir ci-dessus.
PayID	an32	M	ID pour cette transaction attribuée par la plateforme de paiement
Status	a..50	M	OK ou FAILED
Code	n8	M	Code d'erreur conformément au fichier Excel des codes de réponse de la plateforme de paiement
PCNr	n..16	C	Le pseudo-numéro de carte est uniquement retourné pour les types de transactions Authorize ou Sale & CreditEx. Le pseudo-numéro de carte commence avec 0 et les 3 derniers chiffres correspondent à ceux du vrai numéro de carte.

## Gestion des paiements par carte

### Capture

Le commerçant peut choisir différentes options de capture :

- **Manuelle**
- **Automatique**
- **Automatique avec délais personnalisable** (de 1 à 696 heures)

En choisissant le **mode manuel**, il est nécessaire pour le commerçant de valider manuellement chacune des transactions. Le commerçant doit valider la transaction avant 7 jours (délais de garantie des fonds). Les captures manuelles sont possibles via une connexion server-to-server :

<https://paymentpage.axepta.bnpparibas/capture.aspx>

En choisissant le **mode automatique**, la capture se fait automatiquement tous les jours en fin de journée.

En choisissant le **mode automatique avec délais personnalisable**, le commerçant fixe une durée en heure (de 1 à 696) qui correspond à la fréquence de capture à laquelle il souhaite remettre les transactions en banque.

### ***Capture partielle***

Le commerçant peut valider tout ou une partie du montant d'une transaction.

La capture partielle peut se faire :

- Soit via une connexion server-to-server en valorisant le paramètre « Amount » avec le montant partiel à capturer dans la requête de paiement.
- Soit via le back-office en sélectionnant la vue détaillée de la transaction où l'utilisateur pourra choisir le montant à capturer ne dépassant pas le montant total de la transaction.

**Remarque :** pour des raisons de sécurité, la plateforme de paiement rejette toutes les requêtes de paiement avec des erreurs de formatage. Par conséquent, utilisez le type de données approprié pour chaque paramètre.

Le tableau suivant décrit les paramètres de requête de paiement chiffrés :

Paramètre	Format	CND	Description
RefNr	an..12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces)</li> <li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li> <li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> En cas de capture manuelle, la RefNr doit être identique en autorisation (création du paiement) et la capture. Si les valeurs sont différentes, la réconciliation financière ne pourra pas être effectuée.</p> </div>
MerchantID	ans..30	M	Identifiant du commerçant attribué par BNP Paribas
PayID	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement
TransID	ans..64		Identifiant de la transaction devant être unique pour chaque paiement
MAC	an64	MM	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
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	Devise, trois chiffres DIN / ISO 4217
ReqID	ans..32	O	Pour éviter les paiements en double, saisissez une valeur alphanumérique qui identifie votre transaction et ne peut être attribuée qu'une seule fois. Si la transaction est à nouveau soumise avec le paramètre ReqID identique, la plateforme de paiement n'exécute pas le paiement et se contente de retourner le statut de la transaction d'origine. Attention : Plateforme de paiement doit afficher un statut de transaction finalisée pour la première action initiale. Les introductions avec un ReqID identique pour un statut ouvert sont traitées à intervalles réguliers.
FinishAuth	a1	C	Uniquement avec ETM : transmettez la valeur <Y> pour empêcher le renouvellement des autorisations garanties et des montant résiduels à la suite de captures partielles. Veuillez utiliser ce paramètre uniquement si vous utilisez la fonction supplémentaire ETM (Extended Transaction Management).
Textfield1	ans..30	O	Informations sur le porteur de carte (par exemple : nom)

Textfeld2	ans..30	O	Informations sur le porteur de carte (par exemple : ville)
-----------	---------	---	--

Le tableau suivant décrit les paramètres de réponse de la plateforme de paiement :

Paramètre	Format	CND	Description
RefNr	an..12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces)</li> <li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li> <li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li> </ul>
MID	ans..30	M	Identifiant du commerçant
PayID	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement ; p. ex. pour référencement dans les fichiers batch
XID	an32	M	Identifiant pour toutes les transactions uniques (autorisation, capture, remboursement) pour un paiement attribué par la plateforme de paiement
TransID	ans..64	M	Numéro de transaction du commerçant
Status	a..50	M	OK ou FAILED (échec)
Description	ans..1024	M	Détails complémentaires dans le cas où le paiement est rejeté. N'utilisez pas la <b>Description</b> , mais le paramètre <b>Code</b> pour l'analyse du statut de transaction !
Code	n8	M	Code d'erreur selon le fichier Excel des codes de réponses de la plateforme de paiement

A noter : Les captures partielles sont également possibles en valorisant le paramètre « Amount » avec le montant partiel à capturer.

## Annulation

L'annulation permet d'annuler une transaction avant que celle-ci soit remise en banque (capturée, voir paragraphe ci-dessous).

Pour honorer la demande d'annulation, BNP Paribas procède à deux vérifications

- Le montant: il est interdit d'annuler un montant supérieur au montant initial de la transaction.
- Le délai de remise en paiement : le délai est défini au moment de la demande d'autorisation et lorsque ce délai est dépassé la transaction ne peut plus être annulée.

Utilisez l'URL suivante :

<https://paymentpage.axepta.bnpparibas/reverse.aspx>

**Remarque :** Pour des raisons de sécurité, la plateforme de paiement rejette toutes les requêtes de paiement avec des erreurs de formatage. Par conséquent, utilisez le type de donnée approprié pour chaque paramètre.

**Remarque :** Reverse.aspx ne permet pas uniquement d'annuler (reverse) les autorisations, mais toutes les dernières étapes de ces transactions. Si la dernière transaction était une capture, Reverse.aspx initie l'annulation (reverse) (p. ex. un remboursement). Par conséquent, vous devez faire preuve d'une extrême prudence. Utilisez ce paramètre à vos propres risques. Nous vous recommandons de vérifier le statut de transaction avec **Inquire.aspx** avant d'utiliser Reverse.aspx.

(Se référer à la documentation « demande de statut » pour des informations supplémentaires sur inquire.aspx)

Le tableau suivant décrit les paramètres de requête de paiement chiffrés :

Paramètre	Format	CND	Description
MerchantID	ans..30	M	Identifiant du commerçant
PayID	an32	M	Identifiant de la plateforme de paiement pour l'identification du paiement
TransID	ans..64	M	Identifiant de la transaction devant être unique pour chaque paiement

<b>Amount</b>	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).  <div style="border: 1px solid red; padding: 5px; display: inline-block;">  Le montant de l'annulation doit être le même que le montant de l'autorisation. L'annulation partielle n'est pas disponible. </div>
<b>Currency</b>	a3	M	Code de devise, trois chiffres DIN / ISO 4217
<b>MAC</b>	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
<b>ReqID</b>	ans..32	O	Pour éviter les paiements en double, saisissez une valeur alphanumérique qui identifie votre transaction et ne peut être attribuée qu'une seule fois. Si la transaction est à nouveau soumise avec le paramètre ReqID identique, la plateforme de paiement n'exécute pas le paiement et se contente de retourner le statut de la transaction d'origine. Attention : Plateforme de paiement doit afficher un statut de transaction finalisée pour la première action initiale. Les introductions avec un ReqID identique pour un statut ouvert sont traitées à intervalles réguliers.

Le tableau suivant décrit les paramètres de réponse de la plateforme de paiement :

Paramètre	Format	CND	Description
<b>MID</b>	ans..30	MC	Identifiant du commerçant
<b>PayID</b>	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement ; p. ex. pour référencement dans les fichiers batch
<b>XID</b>	an32	M	Identifiant pour toutes les transactions uniques (autorisation, capture, remboursement) pour un paiement attribué par la plateforme de paiement
<b>TransID</b>	ans..64	M	Numéro de transaction du commerçant
<b>Status</b>	a..50	M	OK ou FAILED (échec)
<b>Description</b>	ans..1024	M	Détails complémentaires dans le cas où le paiement est rejeté. N'utilisez pas la <b>Description</b> , mais le paramètre <b>Code</b> pour l'analyse du statut de transaction !
<b>Code</b>	n8	M	Code d'erreur selon le fichier Excel des codes de réponses de la plateforme de paiement

## Remboursement

Le remboursement permet de recrediter un client qui a précédemment été débité (produit non parvenu, indisponible, détérioré, retour... etc.). Le compte du client est crédité du montant remboursé et le compte du commerçant est débité de ce même montant. Le commerçant a la possibilité de rembourser un client jusque dans les 12 mois qui suivent sa commande. Il peut faire autant de remboursements partiels qu'il souhaite tant qu'il ne dépasse pas ce délai de ces 12 mois.

Toute tentative de remboursement sur une transaction impayée sera refusée.

Les remboursements sont possibles via une connexion serveur-to-serveur. La plateforme de paiement autorise les remboursements liés à une capture précédemment activée par la plateforme de paiement, et autorise les commerçants à procéder à des remboursements sans transaction de référence. Cette section décrit l'exécution des remboursements avec des transactions de référence. Si vous vous reportez à une capture pour un remboursement, le montant du remboursement est limité au montant de la capture précédente.

Pour procéder à un remboursement avec une transaction de référence, utilisez l'URL suivante :

<https://paymentpage.axepta.bnpparibas/credit.aspx>

**Remarque :** pour des raisons de sécurité, la plateforme de paiement rejette toutes les requêtes de paiement avec des erreurs de formatage. Par conséquent, utilisez le type de donnée approprié pour chaque paramètre.

Le tableau suivant décrit les paramètres de requête de paiement chiffrés :

Paramètre	Format	CND	Description
-----------	--------	-----	-------------

<b>RefNr</b>	an12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces)</li> <li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li> <li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li> </ul>
<b>MerchantID</b>	ans..30	M	Identifiant du commerçant attribué par BNP Paribas
<b>PayID</b>	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement
<b>TransID</b>	ans..64	M	Identifiant de la transaction devant être unique pour chaque paiement
<b>MAC</b>	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
<b>Amount</b>	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).
<b>Currency</b>	a3	M	Devise, trois chiffres DIN / ISO 4217
<b>OrderDesc</b>	ans..768	O	Numéro de référence du commerçant
<b>ReqID</b>	ans..32	O	Pour éviter les paiements en double, saisissez une valeur alphanumérique qui identifie votre transaction et ne peut être attribuée qu'une seule fois. Si la transaction est à nouveau soumise avec le paramètre ReqID identique, la plateforme de paiement n'exécute pas le paiement et se contente de retourner le statut de la transaction d'origine. Attention : Plateforme de paiement doit afficher un statut de transaction finalisée pour la première action initiale. Les introductions avec un ReqID identique pour un statut ouvert sont traitées à intervalles réguliers.
<b>Textfeld1</b>	ans..30	O	Informations sur le porteur de carte (par exemple : nom)
<b>Textfeld2</b>	ans..30	O	Informations sur le porteur de carte (par exemple : ville)

Le tableau suivant décrit les paramètres de réponse de la plateforme de paiement :

Paramètre	Format	CND	Description
<b>RefNr</b>	an12	OC	Le numéro de référence univoque du commerçant, qui sert de référence de remboursement dans le fichier EPA de l'acquéreur. Veuillez noter que sans la livraison de référence propre à la boutique, vous ne pouvez pas lire la transaction EPA ; quant au fichier de règlement supplémentaire, nous ne pouvons pas ajouter les données de paiement supplémentaires.  Notes: <ul style="list-style-type: none"> <li>• <b>Taille fixe</b> de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, <b>pas de caractères spéciaux</b> comme les espaces)</li> <li>• <b>Pour AMEX</b> : le champ RefNr est <b>obligatoire</b></li> <li>• Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)</li> </ul>
<b>MID</b>	ans..30	M	Identifiant du commerçant
<b>PayID</b>	an32	M	Identifiant attribué par la plateforme de paiement pour le paiement ; p. ex. pour référencement dans les fichiers batch
<b>XID</b>	an32	M	Identifiant pour toutes les transactions uniques (autorisation, capture, remboursement) pour un paiement attribué par la plateforme de paiement
<b>TransID</b>	ans..64	M	Numéro de transaction du commerçant
<b>Status</b>	a..50	M	OK ou FAILED (échec)
<b>Description</b>	ans..1024	M	Détails complémentaires dans le cas où le paiement est rejeté. N'utilisez pas la <b>Description</b> , mais le paramètre <b>Code</b> pour l'analyse du statut de transaction !
<b>Code</b>	n8	M	Code d'erreur selon le fichier Excel des codes de réponses de la plateforme de paiement