

Paieement récurrent (Abonnement) / One click

- [Paieement récurrent \(abonnement\)](#)
 - [Initialisation](#)
 - [Paieement récurrent](#)
- [Paramètres de la requête de paieement récurrent](#)
- [Paieement en un clic](#)
- [Paramètres de la requête de paieement one-click](#)

Paieement récurrent (abonnement)

Le paieement récurrent permet d'effectuer des paieements automatiques à intervalles de temps réguliers.

Pour procéder à un paieement récurrent, le commerçant devra suivre les étapes suivantes :

Initialisation

1. Un premier paieement doit être effectué (appel payssl.aspx) en ajoutant le paramètre RTF=I pour indiquer qu'il s'agit d'un paieement initial.

2. Vous obtenez dans la réponse de cet appel 4 paramètres à stocker :

- PCNr (Pseudo Card Number) : alias/token réutilisable par la suite
- CCBBrand
- CCEXpiry
- schemeReferencelD : Donnée utilisée pour chaîner les transactions récurrentes à la 1ère transaction de l'abonnement

=> Ces quatre paramètres seront nécessaires pour les paieements récurrents qui seront effectués via une requête en Serveur to serveur, c'est-à-dire via direct.aspx, ou bien via paynow.aspx.

Paieement récurrent

3. Lancer une requête direct.aspx avec les paramètres obligatoires (voir tableau des paramètres plus bas dans cette section).

- Les paramètres "CCNr", "CCEXpiry" et "CCBrand" seront ceux récupérés dans la réponse du paieement initial.
- Ajoutez le paramètre "RTF=R" dans chacune de vos transactions récurrentes.
- Ajoutez également le paramètre "Vbv=no", qui vous permettra de forcer la non-utilisation de la procédure d'authentification 3Dsecure
- Enfin, utilisez le champ schemeReferencelD reçu en réponse de la requête de paieement initiale afin de chaîner les transactions à la transaction initiale

Les moyens de paieement permettant de faire du **paieement récurrent (abonnement)** sont les suivants :



Abonnements souscrits avant le 01/01/2022

Les paieements des abonnements par carte souscrits avant le 01/01/2022 doivent également faire l'objet d'un chaînage.

La mise en place de ce chaînage est décrite dans la section [Mise à jour des abonnements - 01/01/2022](#)

Paramètres de la requête de paieement récurrent

Le tableau suivant décrit les paramètres de requête de paiement chiffrés nécessaires pour le paiement récurrent :

Paramètre	Format	CND	Description
MerchantID	ans..30	M	Identifiant du commerçant désigné par BNP Paribas. Ce paramètre doit être transmis non chiffré.
TransID	ans..64	M	Identifiant unique de la transaction
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"> • Taille fixe de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, pas de caractères spéciaux comme les espaces,) • Pour AMEX : le champ RefNr est obligatoire • Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)
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).
Amount3D	n..10	OC	Uniquement pour 3D Secure : montant pour l'authentification avec Verified, SecureCode et SafeKey si le paramètre Amount 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 : Amount3D=12000; Amount=2000 . 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 selon ISO 4217
MAC	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
URLSuccess	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 UserData (Données utilisateur).
URLFailure	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 UserData (Données utilisateur).
Response	a7	O	Réponse de statut envoyée par la plateforme de paiement à URLSuccess et URLFailure , doit être chiffrée. À cette fin, transmettez le paramètre Response=encrypt .
URLNotify	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 UserData .
UserData	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
Capture	ans..6	O	Détermine le type et l'heure de la capture. AUTO : capture immédiate après autorisation (valeur par défaut). MANUAL : capture effectuée par le commerçant. <Number> : délai en heures jusqu'à la capture (nombre de 1 à 696).
OrderDesc	ans..768	M	Description des produits achetés, prix à l'unité, etc.
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.
Plain	ans..50	O	Valeur définie par le commerçant pour retourner certaines informations non chiffrées (p. ex. identifiant du commerçant (MID))
Custom	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
expirationTime	ans..19	O	Date et heure de fin du traitement de la transaction, en heure UTC. Format : AAAA-MM-jjTHH:mm:ss
AccVerify	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

RTF	a1	O	<p>Pour un paiement récurrent (abonnement) :</p> <p>I = paiement initial pour le nouvel abonnement</p> <p>R = paiement récurrent</p>
schemeReferencelD	ans..64	M*	<p>Donnée de chaînage utilisée dans le cadre des abonnements par carte uniquement.</p> <p>Elle permet de chaîner les transactions récurrentes à la première transaction de l'abonnement.</p> <p>Ce champ est obligatoire pour les paiements récurrents (RTF = R) et contient la valeur reçue dans la réponse du paiement d'initialisation de l'abonnement (RTF=I)</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Utiliser uniquement la valeur reçue dans la réponse du paiement d'initialisation de l'abonnement (RTF=I)</p> </div>

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
MID	ans..30	M	Identifiant du commerçant (MerchantID) attribué par BNP Paribas.
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
refnr	an12	OC	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Taille fixe de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, pas de caractères spéciaux comme les espaces) • Pour AMEX : le champ RefNr est obligatoire • Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)
Status	a..50	M	OK / AUTHORIZED (URLSuccess) / FAILED (URLFailure)
Description	ans..1024	M	Détails supplémentaires dans le cas où le paiement est rejeté. N'utilisez pas la Description , mais le paramètre Code pour l'analyse du statut de transaction !
Code	n8	M	Code erreur de réponses de la plateforme de paiement (voir fichier Excel des codes erreur)
MAC	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
UserData	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
PCNr	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.
CCBrand	a..22	OC	Désignation de la marque de carte
CCEpiry	n6	OC	En combinaison avec PCNr : date d'expiration de la carte au format AAAAMM (201706).
maskedpan	an..19	OC	Numéro de carte masqué 6X4
CAVV	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.
ECI	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.
DDD	a1	C	<p>Pour l'hébergement d'authentification 3D Secure :</p> <p>Y - entièrement authentifié (authentification complète effectuée)</p> <p>N - not enrolled (vérifié, mais l'émetteur ne participe pas)</p> <p>U - non éligible (erreur technique)</p> <p>A - attempt (la carte ne participe pas)</p> <p>B - bypass (contournement, uniquement pour CardinalCommerce)</p>

Type	ans..20	C	Pour 3D Secure uniquement, en réponse à URLNotify : abréviation du type de paiement, (exemple : SSL)
Plain	ans..50	O	Une valeur définie par le commerçant pour retourner certaines informations non chiffrées (p. ex. identifiant du commerçant)
Custom	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
CustomField [n]	ans..50	O	Champ pouvant être utilisé individuellement par le commerçant. Actuellement, 9 champs de CustomField1 à CustomField9 sont pris en charge.
schemeReferencelD	ans..64	M	Donnée de chaînage utilisée dans le cadre des abonnements par carte uniquement. Elle permet de chainer les transactions récurrentes (RTF = R) d'un abonnement à la première transaction (RTF = I) Ce champ peut être valorisé dans la réponse d'un paiement récurrent, mais cette valeur n'a pas besoin d'être stockée car elle ne sera pas utilisée.

Paiement en un clic

Le paiement en un clic peut être effectué via la tokenisation. Le token fournit au commerçant un remplacement complet du numéro de carte. Le token est généré par la plateforme, mais conserve les mêmes options et fonctions que le numéro de carte réelle. Cela permet aux commerçants d'éviter d'avoir à obtenir la certification PCI DSS (Payment Card Industry Data Security Standard).

Le client récurrent n'a pas à saisir de nouveau les détails de sa carte et le commerçant peut donc offrir un parcours d'achat fluide et simple à ses clients et augmenter ainsi son taux de conversion.

Pour ce faire, le commerçant doit utiliser le paramètre **PCNr** (Pseudo Card Number) pour autoriser les paiements en un clic. Cela est possible avec le protocole CB2A. Ce paramètre se trouve parmi les paramètres de réponse envoyée par la plateforme de paiement. A noter qu'une première transaction est nécessaire pour la génération du token PCNr que vous pourrez stocker et utiliser pour le paiement suivant. Cette première transaction peut se faire via la page de paiement. La deuxième transaction se fait via une connexion serveur-to-serveur.

Les moyens de paiement permettant de faire du **paiement en un clic (one click)** sont les suivants :



Paramètres de la requête de paiement one-click

Le tableau suivant décrit les paramètres de requête de paiement chiffrés nécessaires pour le paiement one-click:

Paramètre	Format	CND	Description
MerchantID	ans..30	M	Identifiant du commerçant désigné par BNP Paribas. Ce paramètre doit être transmis non chiffré.
TransID	ans..64	M	Identifiant unique de la transaction
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"> • Taille fixe de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, pas de caractères spéciaux comme les espaces,) • Pour AMEX : le champ RefNr est obligatoire • Si le nombre de caractères renseignés est inférieur à 12, alors BNP complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)
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).

Amount3D	n..10	OC	Uniquement pour 3D Secure : montant pour l'authentification avec Verified, SecureCode et SafeKey si le paramètre Amount 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 : Amount3D=12000; Amount=2000 . 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 selon ISO 4217
MAC	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
URLSuccess	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 UserData (Données utilisateur).
URLFailure	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 UserData (Données utilisateur).
Response	a7	O	Réponse de statut envoyée par la plateforme de paiement à URLSuccess et URLFailure , doit être chiffrée. À cette fin, transmettez le paramètre Response=encrypt .
URLNotify	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 UserData .
UserData	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
Capture	ans..6	O	Détermine le type et l'heure de la capture. AUTO : capture immédiate après autorisation (valeur par défaut). MANUAL : capture effectuée par le commerçant. <Number> : délai en heures jusqu'à la capture (nombre de 1 à 696).
OrderDesc	ans..768	M	Description des produits achetés, prix à l'unité, etc.
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.
Plain	ans..50	O	Valeur définie par le commerçant pour retourner certaines informations non chiffrées (p. ex. identifiant du commerçant (MID))
Custom	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
expirationTime	ans..19	O	Date et heure de fin du traitement de la transaction, en heure UTC. Format : AAAA-MM-jjTHH:mm:ss
AccVerify	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
RTF	a1	O	Pour un paiement récurrent (abonnement) : I = paiement initial pour le nouvel abonnement R = paiement récurrent

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
MID	ans..30	M	Identifiant du commerçant (MerchantID) attribué par BNP Paribas.
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

refnr	an12	OC	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Taille fixe de 12 caractères (uniquement des caractères alphabétiques (A..Z, a..z) et numériques (0..9) sont autorisés, pas de caractères spéciaux comme les espaces) • Pour AMEX : le champ RefNr est obligatoire • Si le nombre de caractères renseignés est inférieur à 12, alors BNP Paribas complètera, en partant de la gauche, avec des "0" (Exemple : 000018279568)
Status	a..50	M	OK / AUTHORIZED (URLSuccess) / FAILED (URLFailure)
Description	ans..1024	M	Détails supplémentaires dans le cas où le paiement est rejeté. N'utilisez pas la Description , mais le paramètre Code pour l'analyse du statut de transaction !
Code	n8	M	Code erreur de réponses de la plateforme de paiement (voir fichier Excel des codes erreur)
MAC	an64	M	Code HMAC (Hash Message Authentication Code) avec algorithme SHA-256
UserData	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
PCNr	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.
CCBrand	a..22	OC	Désignation de la marque de carte
CCEpiry	n6	OC	En combinaison avec PCNr : date d'expiration de la carte au format AAAAMM (201706).
maskedpan	an..19	OC	Numéro de carte masqué 6X4
CAVV	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.
ECI	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.
DDD	a1	C	<p>Pour l'hébergement d'authentification 3D Secure :</p> <p>Y - entièrement authentifié (authentification complète effectuée)</p> <p>N - not enrolled (vérifié, mais l'émetteur ne participe pas)</p> <p>U - non éligible (erreur technique)</p> <p>A - attempt (la carte ne participe pas)</p> <p>B - bypass (contournement, uniquement pour CardinalCommerce)</p>
Type	ans..20	C	Pour 3D Secure uniquement, en réponse à URLNotify : abréviation du type de paiement, (exemple : SSL)
Plain	ans..50	O	Une valeur définie par le commerçant pour retourner certaines informations non chiffrées (p. ex. identifiant du commerçant)
Custom	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
CustomField [n]	ans..50	O	Champ pouvant être utilisé individuellement par le commerçant. Actuellement, 9 champs de CustomField1 à CustomField9 sont pris en charge.