Intégration avec Ingenico ePayments DirectLink (serveur à serveur)

ingenico
ePayments

Table des matières

1. Introduction

2. Procédures générales et paramètres de sécurité

2.1 Utilisateur API

2.2 Formulaire de requête

2.3 Sécurité

2.3.1 Cryptage

2.3.2 Adresse IP

2.3.3 Signature SHA

2.4 Parsing de la réponse

3. Effectuer une nouvelle commande

3.1 URL de requête

3.2 Paramètres de requête

3.3 Page de test

3.4 Exclure les moyens de paiement spécifiques

3.5 Requête de commande utilisant 3-D Secure

3.6 Subdivision en cartes de crédit/débit

3.7 Traitement de transactions avec des identifiants enregistrés

4. Réponse de commande

4.1 Double requête (doublon)

5. Maintenance directe: Maintenance sur des commandes existantes

5.1 Requête de maintenance

5.1.1 URL de requête

5.1.2 Paramètres de requête

5.1.3 Page de test

5.2 Réponse de maintenance

5.3 Double requête (doublon)

6. Requête Directe (Direct Query): demander le statut d’une commande

6.1 Demande de requête

6.1.1 URL de requête

6.1.2 Paramètres de requête

6.1.3 Page de test

6.2 Réponse de requête

6.2.1 Transactions traitées en e-Commerce

6.3 Statuts possibles de réponse

6.4 Requête Directe comme sécurité

7. Demande de politique de confidentialité à l’attention du responsable du traitement des données

7.1 Demande de requête

7.1.1 Demande d'URL

7.1.2 Demande de Paramètres

7.1.3 Page de test

7.2 Réponse de requête

8. Exceptions parmi les moyens de paiement

8.1 Direct Debits

8.1.1 Direct Debits AT

8.1.2 Direct Debits DE (ELV)

8.1.3 Direct Debits NL

8.2 Moyen de paiement où seule la maintenance est possible via DirectLink

1. Introduction

Ingenico ePayments DirectLink vous permet d'établir des liens entre vos applications et notre système, comme si notre système était tout simplement un serveur local. Cela fournit un accès programme à programme (serveur à serveur) entre le logiciel du marchand et nos fonctions de paiement et d'administration. Le programme du marchand interagit directement avec notre API à distance, sans intervention humaine.

> En utilisant DirectLink, il n'y a aucun contact entre notre système et le client de notre marchand. Le marchand transmet toutes les informations requises pour effectuer directement le paiement à partir de notre système dans une requête HTTPS POST. Notre système demande la transaction financière (de manière synchrone ou asynchrone) à l'acquéreur pertinent et retourne la réponse au marchand dans un format XML. Le programme du marchand lit la réponse et reprend le traitement.
> Le marchand est donc responsable pour la collecte et le stockage des détails confidentiels de paiement de son client. Il doit garantir la confidentialité et la sécurité de ces détails via l'utilisation de communication web encryptée et d'un serveur de sécurité.

Le marchand peut effectuer des nouvelles commandes, des maintenances sur des commandes existantes et des interrogations sur le statut d'une commande en particulier en utilisant DirectLink.

L'usage de requêtes automatisées en DirectLink par le marchand ne l'empêche pas de consulter manuellement l'historique des transactions dans son module de gestion, en utilisant son navigateur internet ou un téléchargement de rapport. Pour la configuration et le fonctionnement du site d'administration, veuillez vous référer au Utilisez votre compte Ingenico ePayments / Consultez vos transactions.

2. Procédures générales et paramètres de sécurité

Les procédures générales et contrôles de sécurité sont valides pour toutes les demandes DirectLink: nouvelles requêtes de commande, requêtes de maintenance et interrogations directes (direct queries).

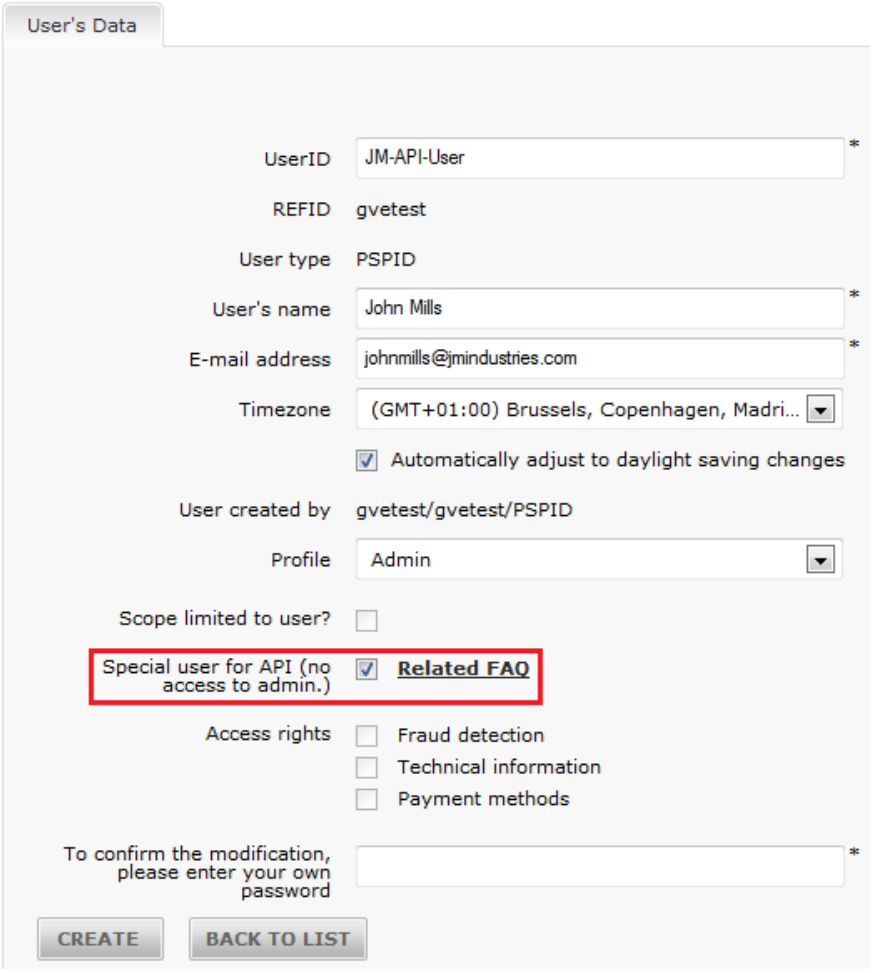
2.1 Utilisateur API

Un utilisateur API (Application Program Interface) est nécessaire pour présenter des demandes DirectLink.

En général, cet utilisateur est spécifiquement conçu pour qu'une application puisse présenter des demandes automatiques à la plateforme de paiement.

Vous pouvez créer un utilisateur API dans votre compte Ingenico via « Configuration » > « Users » (Utilisateurs). Sélectionnez « New User » (Nouvel utilisateur) et remplissez les champs obligatoires.

Pour que le nouvel utilisateur soit un utilisateur API, assurez-vous de cocher la case « Special user for API (no access to admin.) » (Utilisateur spécial API (aucun accès admin.)).



Bien que plusieurs profils d'utilisateur soient disponibles pour l'utilisateur API, nous vous recommandons vivement de configurer cet

utilisateur sur le profil « Admin » (Administrateur).
Si vous souhaitez limiter les droits de maintenance des transactions (remboursement, annulations, etc.), vous pourrez toujours modifier le profil utilisateur et le configurer sur « Encoder » (Encodeur), par exemple.

En cas de doute, nous vous recommandons de choisir le profil « Admin », autrement, accédez à Profils d'utilsateur (Gestionnaire des utilisateurs).

Le mot de passe d'un utilisateur API n'a pas besoin d'être modifié régulièrement. Ce qui est avantageux lorsque le mot de passe doit être codé en dur dans votre application. Nous vous recommandons néanmoins de changer de mot de passe de temps à autre.

Pour en savoir plus sur les types d'utilisateur et sur la façon de modifier le mot de passe de l'utilisateur API, accédez à Types d'utilisateur (Gestionnaire des utilisateurs).

2.2 Formulaire de requête

Pour les requêtes de nouvelle commande, les requêtes de maintenance et les interrogations directes (direct queries), le marchand doit envoyer des requêtes avec certains paramètres vers des URLs spécifiques. Les paramètres de paiement/maintenance/interrogation doivent être envoyés dans une demande POST comme suit:

PSPID=value1&USERID=value2&PSWD=value3&...

Le sous-type (subtype) indiquant le type de média dans le champ header “Content-Type entity” dans la requête POST doit être encodé en "application/x-www-form-urlencoded".

DirectLink fonctionne dans un mode “une requête-une réponse”, chaque paiement est traité individuellement. Notre système gère individuellement les requêtes de transaction via DirectLink et peut travailler simultanément (lorsque cette option est supportée techniquement), par exemple nous attendons la réponse de la banque avant de renvoyer une réponse XLM vers la requête.

2.3 Sécurité

Lorsque nous recevons des requêtes sur nos serveurs, nous vérifions le niveau de cryptage ainsi que l'adresse IP à partir de laquelle la requête a été envoyée.

2.3.1 Cryptage

DirectLink est construit sur un protocole de communication sécurisé et robuste. L'API DirectLink est un ensemble d'instructions soumises avec des requêtes HTTPS POST classiques.

Au niveau du serveur, nous utilisons un certificat délivré par Verisign. Le cryptage TLS garantit que ce sont effectivement nos serveurs avec lesquels vous communiquez et que vos données sont transmises sous une forme encryptée. Il n'est pas nécessaire d'utiliser un certificat client TLS.

Lorsque nous recevons une requête, nous vérifions le niveau de cryptage. Nous permettons aux marchands de se connecter à nous dans un seul mode https sécurisé en utilisant les protocoles TLS et nous recommandons fortement l'utilisation des versions les plus récentes et sécurisées, qui sont actuellement TLS 1.1 et 1.2.

Note: A l'heure où nous avons écrit cette documentation, nous supportions toujours SSL v3. Cependant, dû à certaines vulnérabilités, ce protocole est en train d'être progressivement décommissionné et ne sera bientôt plus supporté.

2.3.2 Adresse IP

Pour chaque requête, notre système vérifie l'adresse IP à partir de laquelle la requête a été envoyée afin de s'assurer que les requêtes ont bien été envoyées à partir du serveur du marchand. Dans le champ adresse IP de l'onglet "Contrôle de données et d'origine”, dans la

section "Contrôles pour DirectLink" de la page Information technique de votre compte, vous devez entrer l'adresse IP ou le groupe d'adresse IP des serveurs qui envoient vos requêtes.

Si l'adresse IP à partir de laquelle la requête a été envoyée n'a pas été déclarée dans le champ d'adresse IP de l'onglet "Contrôle de données et origine", à vérifier dans la section DirectLink de la page d'information technique de votre compte, vous recevrez le message d'erreur "unknown order/1/i". L'adresse IP à partir de laquelle la requête a été envoyée sera également montrée dans le message d'erreur.

2.3.3 Signature SHA

La signature SHA est basée sur le principe même que le serveur du marchand génère une chaîne unique de caractères pour chaque commande, hachée avec les algorythmes SHA-1, SHA-256 u SHA-512. Le résultat de ce hachage nous est envoyé dans la requête de commande du marchand. Notre système reconstruit la signature afin de vérifier l'intégrité des données de commande qui nous ont été envoyées dans la requête.

Cette chaîne est construite en concaténant les valeurs des champs envoyés avec la commande (triés alphabétiquement, dans le format 'paramètre=valeur'), avec chaque paramètre et valeur suivis d'une passphrase. La passphrase est définie dans l'Information Technique du marchand, dans l'onglet "Contrôle de données et origine", dans la section "Contrôles pour DirectLink". Pour la liste complete des paramètres à inclure dans le Digest SHA, veuillez cliquer ici. A noter que ces valeurs sont toutes sensibles à la casse lorsqu'elles sont assemblées pour former la chaîne avant le hachage!

Important

- Tous les paramètres que vous envoyez (et qui apparaissent dans la Liste des Paramètes à inclure dans le calcul du SHA-IN), seront inclus dans la suite (string) à hacher.
- Tous les noms de paramètres devraient être en MAJUSCULES (Afin d'éviter toute confusion)
- Les paramètres doivent être triés par ordre alphabétique
- Les paramètres qui n'ont pas de valeur ne devraient PAS être inclus dans la suite (string) à hacher
- Lorsque vous optez pour le transfert du compte de test en production en utilisant le lien dans votre compte, une passphrase SHA-IN aléatoire sera automatiquement configurée dans votre compte de production.
- **Par mesure de sécurité, nous vous invitons à utiliser des mots de passe SHA différents en TEST et PROD. Veuillez noter que si identiques dans les deux environnements, votre passphrase en TEST serait changée par notre système (vous en seriez bien entendu notifié).**

Lorsque vous hachez la suite (string) composé par l'algorythme SHA, un résumé hexadécimal sera renvoyé. La longueur de ce résumé SHA est de 40 caractères pour le SHA-1, 64 pour le SHA-256 et 128 pour le SHA-512. Ce résultat devrait être envoyé à notre système dans votre requête de commande, en utilisant le champ "SHASign".

Notre système recomposera lui-même la suite (string) SHA en se basant sur les paramètres reçus et comparera le résumé (digest) du marchand avec le résumé (digest) que nous avons généré. Si le résultat n'est pas identique, la commande sera refuse. Ce contrôle garantit l'exactitude et l'intégrité des données de commande.

Vous pouvez tester votre signature SHA ici.

Exemple de calcul d'un SHA-1-IN avec les seuls paramètres de base

Paramètres (par ordre alphabétique)
AMOUNT: 15.00 -> 1500
CARDNO: 4111111111111111
CURRENCY: EUR
OPERATION: RES
ORDERID: 1234
PSPID: MyPSPID

SHA Passphrase (Dans "Information Technique"):
Mysecretsig1875!?

String à hacher
AMOUNT=1500Mysecretsig1875!?CARDNO=4111111111111111Mysecretsig1875!?CURRENCY=EURMysecretsig1875!?
OPERATION=RESMysecretsig1875!?ORDERID=1234Mysecretsig1875!?PSPID=MyPSPIDMysecretsig1875!?

Résumé de résultat (SHA-1)
2B459D4D3AF0C678695AE77EE5BF0C83CA6F0AD8

Si le signature SHA envoyé dans votre requête ne correspond pas au SHASIGN que nous avons récupéré en utilisant les details de la commande ainsi que la passphrase entrée dans le champ Signature SHA-IN dans l'onglet "Contrôle de données et origine", dans la section "Contrôles pour DirectLink" dans la page d'Information Technique, vous recevrez le message d'erreur "unknown order/1/s/".

Si le champ "SHASIGN" dans votre requête est vide, mais qu'une passphrase a été entrée dans le champ Signature SHA-IN dans l'onglet "Contrôle de données et origine", dans la section "Contrôles pour DirectLink" dans la page d'Information Technique (indiquant ainsi que vous voulez utilise une signature SHA pour chaque transaction), vous recevrez le message d'erreur "unknown order/0/s/".

2.4 Parsing de la réponse

Nous retournerons une réponse XML à votre requête. Veuillez vous assurer que vos systèmes sont bien en mesure de faire du parsing en recevant la réponse XML de manière aussi tolérante que possible afin d'éviter tout problème dans le futur, par exemple éviter les noms d'attributs sensibles à la casse, ne pas convenir d'un ordre spécifique pour les attributs retournés dans les réponses, s'assurer que les nouveaux attributs dans la réponse ne causeront pas de problème, etc.

3. Effectuer une nouvelle commande

3.1 URL de requête

- L'URL de la requête dans l'environnement de TEST est https://ogone.test.v-psp.com/ncol/test/orderdirect.asp.
- L'URL de la requête dans l'environnement de PRODUCTION est https://secure.ogone.com/ncol/prod/orderdirect.asp.

Remplacer "test" par "prod"

N'oubliez pas de remplacer "test" par "prod" dans l'URL de la requête lorsque vous passez à votre compte de PRODUCTION. Si vous oubliez de changer l'URL de requête, lorsque vous commencerez à traiter des commandes réelles, vos transactions seront envoyées vers l'environnement de test et ne seront pas envoyées vers les acquéreurs/banques.

3.2 Paramètres de requête

Le tableau ci-dessous contient les paramètres de requête nécessaires à l'envoi d'une nouvelle commande:

Format: AN= Alphanumérique / N=Numérique, le nombre maximum de caractères autorisés

Champ	Usage	Format	Obligatoire
PSPID	Votre nom d'affiliation dans notre système.	AN, 30	Oui
ORDERID	Votre numéro de commande unique (référence marchand).	AN, 40	Oui
USERID	Nom de votre utilisateur applicatif (API). Veuillez vous référer à la documentation User Manager pour plus d'informations sur comment créer un utilisateur API.	AN, 20 (min 2)	Oui
PSWD	Mot de passe de l'utilisateur API (USERID).	AN	Oui
AMOUNT	Montant à payer MULTIPLIE PAR 100, puisque le format du montant ne doit pas contenir de décimales or tout type de séparateur.	N, 15	Oui
CURRENCY	Code devise de la commande en format ISO alpha, par exemple: EUR, USD, GBP, CHF, etc.	AN, 3	Oui
CARDNO	Numéro de Carte/Compte.	AN, 21	Oui
ED	Date d'expiration.	MM/AA ou MMAA	Oui
COM	Description de la Commande.	AN, 100	Non
CN	Nom du client.	AN, 35	Non
EMAIL	Adresse e-mail du client.	AN, 50	Non
SHASIGN	Signature (suite (string) hachée) pour authentifier les données (cfr. SHA-IN Signature).	AN, 128	Non

Champ	Usage	Format	Obligatoire
CVC	Code de Vérification de la Carte (CVC - Card Verification Code). En fonction du type de carte, le code de vérification sera un code de 3 ou 4 chiffres, situé à l'avant ou à l'arrière de la carte, un numéro d'émission, une date de début ou une date de naissance.	N, 5	Yes
ECOM_PAYMENT_ CARD_VERIFICATION	Alternative au CVC: date de naissance / numéro d'émission / etc. (en function du pays/de la banque)	N, 5	Oui
OWNERADDRESS	Nom de rue et numéro du client.	AN, 50	Non
OWNERZIP	Code postal du client.	AN, 10	Non
OWNERTOWN	Nom de la ville du client.	AN, 40	Non
OWNERCTY	Pays du client, par exemple BE, NL, FR, etc.	AN, 2	Non
OWNERTELNO	Numéro de téléphone du client.	AN, 30	Non
OPERATION	Définit le type de transaction demandée. Vous pouvez configurer une opération par défaut (procédure de paiement) dans l'onglet "Paramètres de transaction globaux", section "Code d'opération par défaut" de la page d'Information technique. Lorsque vous envoyez une valeur d'opération dans la requête, celle-ci écrasera la valeur par défaut. Valeurs possibles: • RES : demande d'autorisation • SAL : demande de vente directe • RFD: remboursement, non lié à un paiement précédemment effectué, donc pas une opération de maintenance sur une transaction existante (vous ne pouvez pas utilise cette opération sans permission spécifique de votre acquéreur). Optionnel: • PAU: demande de pré-autorisation: En accord avec votre acquéreur vous pouvez utiliser ce code d'opération pour réserver temporairement des fonds sur la carte d'un client. Ceci est une pratique courante dans les industries liées au voyage et à la location. Le code PAU/pré-autorisation ne peut actuellement être utilisé que pour les transactions MasterCard et n'est supporté que par quelques acquéreurs. Ce code d'opération ne peut pas être défini comme valeur par défaut dans votre compte Ingenico ePayments. Si vous deviez utiliser le code PAU pour des transactions avec des acquéreurs ou des types de carte qui ne supportent pas la pré-autorisation, ces transactions ne seraient pas bloquées, mais traitées comme des autorisations classiques (RES).	A, 3	Oui
WITHROOT	Ajoute un élément racine à votre réponse XML. Valeurs possibles: 'Y' ou vide.	Y ou <empty>	Non

Champ	Usage	Format	Obligatoire
REMOTE_ADDR	Adresse IP du client (Seulement pour le module de détection de fraude (FDM). Si une vérification de pays ne doit pas être effectuée sur l'adresse IP, envoyez "NONE".	AN	Non
RTIMEOUT	Timeout de requête pour la transaction (en secondes, valeur entre 30 et 90) Important: La valeur que vous configurez ici doit être inférieure à la valeur du timeout dans votre propre système!	N, 2	Non
ECI	Indicateur Electronique de Commerce (Electronic Commerce Indicator). Vous pouvez configurer une valeur ECI par défaut dans l'onglet "Paramètres de transaction globaux", section "valeur ECI par défaut" de la page d'Information Technique. Lorsque vous envoyez une valeur ECI dans la requête, celle-ci écrasera la valeur ECI par défaut. Valeurs (numériques) possibles: 0 - Carte passée dans le terminal 1 - Vente à distance classique (MOTO) (carte non présente) 2 - Paiements périodiques provenant de VAD 3 - Paiements étalés 4 - Entrée manuelle, carte présente 7 - E-commerce avec chiffrement SSL 9 - Paiements périodiques issus du e-commerce	N, 2	Non

Les paramètres suivants sont pertinents dans le cadre des directives Credential on file (COF) pour le paiement en Visa/MasterCard. Des informations détaillées sur leur usage peut être trouver dans un chapitre dédié "Traitement de transactions avec des identifiants enregistrés".

COF_INITIATOR	Credential-on-file initiator Valeurs possibles: • CIT: Une transaction initiée par un titulaire de carte • MIT: Une transaction initiée par un marchand	AN	No
COF_SCHEDULE	Credential-on-files planifiée (ou non planifiée) Valeurs possibles: • SCHED: Une transaction planifiée • UNSCHED: Une transaction non planifiée	AN	No
COF_TRANSACTION	Credential-on-file transaction Valeurs possibles: • FIRST: Première transaction d'une série de transactions • SUBSEQ: Transactions suivantes d'une série de transactions	AN	No

COF_RECURRING_EXPIRY	Date de fin: dernière date de paiement d'une série de paiements récurrents	Date AAAAMMJJ (ex. 20190914)	No
COF_RECURRING_FREQUENCY	Nombre de jours séparant les paiements d'une série.	Chiffres entre 2 et 4 (31, 031 ou 0031)	No

La liste des paramètres possible à envoyer peut être plus longue pour les marchands qui ont actives certaines options/fonctionnalités dans leurs comptes. Veuillez vous référer à la documentation relative à chaque option pour plus d'informations concernant les paramètres additionnels liés à cette option.

Les paramètres de requêtes suivants sont obligatoires pour les nouvelles commandes:

- PSPID et USERID
- PSWD
- ORDERID
- AMOUNT (x 100)
- CURRENCY
- CARDNO
- ED
- CVC
- OPERATION

3.3 Page de test

Une page de test pour une nouvelle commande peut être trouvée à l'adresse: https://ogone.test.v-psp.com/ncol/test/testodl.asp.

3.4 Exclure les moyens de paiement spécifiques

Si vous désirez qu'un client ne soit pas en mesure de payer en utilisant un ou plusieurs moyens de paiement, vous pouvez utiliser un paramètre à cet effet.

Ceci est particulièrement utile pour les sous-types de carte, spécialement lorsque vous désirez accepter un type de carte (ex.: MasterCard), mais pas les sous-types qui lui sont associés (ex.: Maestro).

Le paramètre est le suivant:

Champ	Usage
EXCLPMLIST	Liste des moyens de paiement et/ou types de carte de crédit qui ne doivent PAS être utilisés, séparés par un ";" (point virgule).

Si un client essaie de payer avec une carte liée à un moyen de paiement et/ou un (sous) type de carte que vous avez exclu en utilisant le paramètre EXCLPMLIST, le message d'erreur "Card number incorrect or incompatible" (Numéro de carte incorrect ou incompatible) sera retourné dans le champ NCERRORPLUS.

3.5 Requête de commande utilisant 3-D Secure

Notre système supporte l'usage de 3-D Secure à travers DirectLink.

Important

- Si vous désirez utiliser 3-D Secure avec DirectLink, vous devez obligatoirement avoir l'option D3D activée dans votre compte.

- Certaines banques acquéreurs exigent l'utilisation du 3-D Secure. Veuillez vérifier avec votre acquéreur si tel est le cas pour vous.

3.6 Subdivision en cartes de crédit/débit

La fonctionnalité consistant à subdiviser VISA et MasterCard en méthodes de paiement par débit et par crédit vous permet de les offrir à vos clients sous deux formes (p. ex. VISA Debit et VISA Credit), mais vous pouvez aussi décider de n'accepter qu'une seule de ces deux formes de paiement.

Pour pouvoir utiliser cette fonctionnalité de subdivision en cartes de crédit et de débit via DirectLink, vous devez inclure le paramètre CREDITDEBIT dans les champs masqués que vous envoyez à la page de paiement (et les inclure également, par conséquent, dans le calcul SHA-IN !).

Champ	Format
CREDITDEBIT	"C": credit card (carte de crédit) "D": debit card (carte de débit)

Erreur liée : Si l'acheteur sélectionne la méthode par carte de débit, mais entre ensuite un numéro de carte de crédit, un code d'erreur est renvoyé : « Marque/mode de paiement incorrect ».

Si le paiement est traité avec succès avec le paramètre CREDITDEBIT, ce même paramètre est également renvoyé dans la réponse XML, et / ou peut être demandé avec une requête directe. Cependant, si les valeurs soumises sont C ou D, les valeurs de retour sont « CREDIT » ou « DEBIT ».

Vous trouverez également ces valeurs de retour dans la vue d'ensemble de la transaction via « View transactions » et « Financial history », ainsi que dans les rapports que vous pouvez télécharger ensuite.

Configuration au sein de votre compte

La fonctionnalité de subdivision peut également être activée et configurée par méthode de paiement dans votre compte Ingenico ePayments. Accédez à Subdivision en cartes de crédit/débit pour plus d'informations.

3.7 Traitement de transactions avec des identifiants enregistrés

Les transactions avec identifiants enregistrés (Credential-on-file ou COF en anglais) utilisent les informations relatives à la carte déjà enregistrées par les marchands pour traiter le paiement. Avant d'initier une transaction avec identifiants enregistrés (COF), le titulaire de carte devra d'abord autoriser le marchand à stocker les informations relatives à la carte. Les transactions avec identifiants enregistrés (COF) s'appliquent essentiellement aux paiements récurrents et indiquent si le paiement est initié par le titulaire de carte ou le marchand.

Il existe deux types de transactions avec des identifiants enregistrés (COF) : les transactions initiées par le titulaire de carte (CIT) et les transactions initiées par le marchand (MIT). Une transaction initiée par le titulaire de carte (CIT) devra toujours avoir lieu avant de réaliser des transactions initiées par le marchand (MIT).

Une transaction initiée par le titulaire de carte (CIT) est une transaction dans laquelle le titulaire de carte est impliqué dans la transaction et authentifie personnellement la transaction au moyen d'une signature, de l'outil 3D-Secure ou en montrant une pièce d'identité.

Exemple de transaction initiée par le titulaire de carte (CIT):

Un titulaire de carte achète un billet de train et effectue un paiement. Il ou elle réalise le paiement avec sa carte de crédit et on lui demande

d'authentifier et d'autoriser le paiement. On demande également au titulaire de carte s'il ou elle souhaite que les informations relatives à sa carte de crédit concernant ce paiement soient enregistrées. Si le titulaire de carte accepte, ces informations peuvent ensuite être réutilisées lors de transactions ultérieures initiées par le marchand.

Une transaction initiée par le marchand (MIT) sert de suivi à une transaction initiée par le titulaire de carte (CIT) et d'ordre permanent préautorisé pour les biens et services achetés par le titulaire de carte. Le titulaire de carte ne doit pas être impliqué dans la transaction.

Exemple de transaction initiée par le marchand (MIT):

Un marchand peut initier automatiquement une transaction pour réaliser le paiement d'un titulaire de carte dans le cadre d'un abonnement mensuel à un magazine.

Conformément aux réglementations mises en place par Visa et MasterCard pour les transactions avec identifiants enregistrés (COF), de nouveaux paramètres doivent être envoyés pour définir la transaction COF.

Vous serez concerné si:

- Vous utilisez un pseudonyme (Alias)
- Vous avez l'intention d'initier des transactions récurrentes (planifiées ou non) après avoir initié une transaction initiée par le titulaire de carte (CIT) pour la première fois

Mesures à prendre

Par défaut, les paramètres suivants sont utilisés lors d'une transaction DirectLink Server-to-Server:

Valeurs de paramètres COF_INITIATOR-COF_TRANSACTION-COF_SCHEDULE	Description
CIT-FIRST-UNSCHED	S'applique en cas d'utilisation d'un pseudonyme ou lors de sa création
CIT-FIRST-SCHED	S'applique à un premier paiement planifié/abonnement
MIT-SUBSEQ-UNSCHED	S'applique aux transactions récurrentes
MIT-SUBSEQ-SCHED	S'applique aux paiements échelonnés

Les valeurs par défaut sont sélectionnées si vous n'ajoutez aucun paramètre. Cependant, si vous souhaitez les modifier, vous pouvez changer ces valeurs par défaut en envoyant les nouveaux paramètres. N'oubliez pas de recalculer la signature SHA également (**cliquez ici** pour plus d'informations concernant la signature SHA).

Paramètres	Valeurs	Description
COF_INITIATOR	CIT	Une transaction initiée par un titulaire de carte
	MIT	Une transaction initiée par un marchand
COF_SCHEDULE	SCHED	Une transaction planifiée
	UNSCHED	Une transaction non planifiée
COF_TRANSACTION	FIRST	Première transaction d'une série de transactions

Paramètres	Valeurs	Description
	SUBSEQ	Transactions suivantes d'une série de transactions
COF_RECURRING_EXPIRY	Date AAAAMMJJ (ex. 20190914)	Date de fin: dernière date de paiement d'une série de paiements récurrents
COF_RECURRING_FREQUENCY	Chiffres entre 2 et 4 (31, 031 ou 0031)	Nombre de jours séparant les paiements d'une série.

4. Réponse de commande

Notre serveur retourne une réponse XML à la requête:

Exemple d'une réponse XML à une requête de commande

```
<?xml version="1.0"?>
<ncresponse orderID="99999" PAYID="1111111" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345"
STATUS="5" ECI="7" amount="125" currency="EUR" PM="CreditCard" BRAND="VISA"/>
```

Le tableau ci-dessous contient une liste des attributs de tag de type ncresponse:

Champ	Usage
ACCEPTANCE	Code de réception retourné par l'acquéreur.
amount	Montant de la commande (non multiplié par 100).
BRAND	Card brand or similar information for other payment methods.
currency	Devise de la commande.
ECI	Indicateur Electronique de Commerce.
NCERROR	Code d'erreur.
NCERRORPLUS	Explication du code d'erreur.
NCSTATUS	Statut lié au code NCERROR
orderID	Votre référence de paiement.
PAYID	Référence de paiement dans notre système.
PM	Moyen de paiement.
STATUS	Statut de la transaction. (Statuts possibles)

La liste des attributs peut être plus longue pour les marchands qui ont activés certaines options (par exemple, le module de détection de fraude) dans leurs comptes. Veuillez vous référer à la documentation relative à chaque option pour plus d'informations concernant les attributs de réponses additionnels liés à cette option.

4.1 Double requête (doublon)

Si vous effectuez une requête pour un orderID existant et ayant déjà été utilisé (et traité correctement), notre réponse XML contiendra le PAYID correspondant à l'orderID existant, la valeur ACCEPTANCE donnée par l'acquéreur lors du traitement précédent, le STATUS (statut) "0" ainsi que le NCERROR "50001113".

5. Maintenance directe: Maintenance sur des commandes existantes

Une requête de maintenance directe envoyée de votre application vous permet de:

- effectuer automatiquement une saisie de données (paiement) d'une commande autorisée (plutôt que manuellement dans votre module de gestion (back-office))
- annuler une autorisation liée à une commande
- renouveler une autorisation liée à une commande
- rembourser une commande payée.

Les saisies de données, annulations d'autorisation et renouvellements d'autorisation sont réservés spécifiquement aux marchands qui ont configuré leur compte/requêtes pour effectuer des autorisations et des saisies de données en deux étapes.

5.1 Requête de maintenance

5.1.1 URL de requête

- l'URL de requête dans l'environnement de TEST est https://ogone.test.v-psp.com/ncol/test/maintenancedirect.asp.
- l'URL de requête dans l'environnement de PRODUCTION est https://secure.ogone.com/ncol/prod/maintenancedirect.asp.

Important

N'oubliez pas de remplacer "test" par "prod" dans l'URL de la requête lorsque vous passez à votre compte de PRODUCTION. Si vous oubliez de changer l'URL de requête, lorsque vous commencerez à traiter des commandes réelles, vos transactions seront envoyées vers l'environnement de test et ne seront pas envoyées vers les acquéreurs/banques.

5.1.2 Paramètres de requête

Le tableau ci-dessous comprend les paramètres de requête obligatoires afin d'effectuer une opération de maintenance:

Champ	Usage
AMOUNT	Montant de la commande multiplié par 100. Celui-ci est seulement obligatoire lorsque le montant de la maintenance diffère du montant de l'autorisation initiale. Cependant, nous recommandons son utilisation dans tous les cas. Notre système vérifiera que le montant de la transaction de maintenance n'est pas supérieur au montant de l'autorisation/du paiement.
OPERATION	Valeurs possibles: • REN: renouvellement d'autorisation, si l'autorisation originale n'est plus valide. • DEL: annulation d'autorisation, en laissant la transaction ouverte pour d'autres opérations de maintenance potentielles. • DES: annulation d'autorisation, en clôturant la transaction après cette opération. • SAL: saisie de données partielle (paiement), en laissant la transaction ouverte pour d'autres saisies de données potentielles. • SAS: (dernière) saisie partielle ou totale de données (paiement), en clôturant la transaction (pour d'autres saisies de données) après la saisie de données. • RFD: remboursement partiel (d'une commande payée), en laissant la transaction ouverte pour d'autres remboursements potentiels • RFS: (dernier) remboursement partiel ou total (d'une commande payée), en clôturant la transaction après ce remboursement. A noter que les opérations DEL et DES (annulations d'une autorisation) ne sont pas supportées par tous les acquéreurs, nous enverrons malgré tout une simulation d'annulation d'autorisation dans le module de gestion (back-

Champ	Usage
	office).
ORDERID PAYID	Vous pouvez envoyer le PAYID ou l'ORDERID afin d'identifier la commande originale. Nous recommandons l'utilisation du PAYID.
PSPID	PSPID de votre compte Ingenico ePayments
PSWD	Le mot de passe du USERID
SHASIGN	Calcul de hachage SHA, pour authentifier les données (cfr. Signature SHA-IN)
USERID	Utilisateur API

5.1.3 Page de test

Un exemple (page de test) d'une demande de maintenance directe peut être trouvé à l'adresse: https://ogone.test.v-psp.com/ncol/test /testdm.asp

5.2 Réponse de maintenance

Notre serveur retourne une réponse XML à la requête:

Exemple d'une réponse XML à une requête de maintenance directe:
<?xml version="1.0"?>
<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="91" amount="125" currency="EUR"/>

Le tableau ci-dessous comprend les attributs de tag ncresponse:

Champ	Usage
ACCEPTANCE	Code d'acceptance renvoyé par l'acquéreur
AMOUNT	Montant de la commande (non multiplié par 100)
CURRENCY	Devise de la commande
NCERROR	Code d'erreur
NCERRORPLUS	Explication du code d'erreur (NCERROR)
NCSTATUS	Statut lié au code NCERROR
ORDERID	Votre référence de commande
PAYID	Référence de paiement dans notre système
PAYIDSUB	L'ID de niveau dans l'historique des opérations de maintenance du PAYID

Champ	Usage
STATUS	Statut de la transaction (Statuts possibles)

L'attribut de tag standard pour ncresponse sont identiques à ceux pour la réponse XML à une nouvelle commande, à l'exception de l'attribut additionnels PAYIDSUB.

5.3 Double requête (doublon)

Si la maintenance est demandée deux fois pour la même commande, la seconde demande sera théoriquement refusée avec une erreur "50001127" (cette commande n'est pas autorisée), parce que la transaction initiale approuvée aura déjà modifié le statut de la commande.

6. Requête Directe (Direct Query): demander le statut d'une commande

Une demande d'interrogation directe (direct query) à partir de votre application vous permet de demander le statut d'une commande automatiquement (plutôt que manuellement dans votre module de gestion (back-office)). Vous ne pouvez envoyer des interrogations qu'une à la fois, et ne recevrez qu'un nombre limité de données par rapport à cette commande.

Si vous désirez plus d'informations sur la commande, vous pouvez vérifier la transaction dans le module de gestion (back-office) ou effectuer un téléchargement de fichier automatique ou manuel (cf. Consultez vos transactions et guide d'intégration avancé Batch).

6.1 Demande de requête

6.1.1 URL de requête

- L'URL de requête dans l'environnement de TEST est https://ogone.test.v-psp.com/ncol/test/querydirect.asp
- L'URL de requête dans l'environnement de PRODUCTION est https://secure.ogone.com/ncol/prod/querydirect.asp

Important

N'oubliez pas de remplacer "test" par "prod" dans l'URL de requête lorsque vous passez votre compte en PRODUCTION.

6.1.2 Paramètres de requête

Le tableau ci-dessous comprend les paramètres de requête obligatoires pour effectuer une interrogation directe (direct query):

Champ	Usage
ORDERID	Vous pouvez envoyer le PAYID ou l'ORDERID afin d'identifier la commande originale. Nous recommandons l'utilisation du PAYID.
PAYID	
PAYIDSUB	Vous pouvez indiquer l'ID de niveau d'historique si vous utilise le PAYID pour identifier la commande originale (optionnel).
PSPID	PSPID de votre compte Ingenico ePayments
PSWD	Mot de passe de votre utilisateur API
USERID	Votre utilisateur API

6.1.3 Page de test

Un exemple (page de test) d'une requête d'interrogation directe (') peut être trouvé à l'adresse: https://ogone.test.v-psp.com/ncol/test /testdq.asp.

6.2 Réponse de requête

Notre serveur renvoie une réponse XML à la requête:

Exemple d'une réponse XML response à une interrogation directe (direct query):

```
<?xml version=”1.0”?>
<ncresponse orderID=”99999” PAYID=”1111111” PAYIDSUB=”3” NCSTATUS=”0” NCERROR=”” NCERRORPLUS=””
ACCEPTANCE=”12345” STATUS="9" ECI=”7” amount="125" currency="EUR" PM="CreditCard" BRAND="VISA"
CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55"/>
```

Le tableau ci-dessous comprend une liste des attributs de tag “ncresponse”:

Champ	Usage
ACCEPTANCE	Code d’acceptance renvoyé par l’acquéreur
amount	Montant de la commande (non multiplié par 100)
BRAND	Type de carte ou information similaire pour d’autres moyens de paiement
CARDNO	Le numéro de carte de credit masqué
currency	Devise de la commande
ECI	Indicateur de Commerce Electronique (Electronic Commerce Indicator)
IP	Adresse IP du client, telle que détectée par notre système dans une intégration en mode 3 tiers, ou envoyée via une intégration en mode 2 tiers
NCERROR	Code d’erreur
NCERRORPLUS	Explication du code d’erreur
NCSTATUS	Statut lié au code NCERROR
orderID	Votre référence de commande
PAYID	Référence de paiement dans notre système
PAYIDSUB	L’ID de niveau dans l’historique des opérations de maintenance du PAYID
PM	Moyen de paiement
STATUS	Statut de la transaction

Les paramètres du champ standards libellés ncresponse sont identiques à ceux pour la réponse XML à une nouvelle commande, à l’exception des attributs additionnels PAYIDSUB, CARDNO et IP.

La liste des paramètres peut être plus longue pour les marchands qui ont activé certaines options (par exemple le module de détection de fraude) dans leurs comptes. Veuillez vous référer à la documentation spécifique à l’option pour obtenir plus d’informations sur les paramètres de réponse additionnels liés à ces options.

6.2.1 Transactions traitées en e-Commerce

Si les transactions pour lesquelles vous désirez vérifier le statut ont été traitées en mode e-Commerce, vous recevrez également les attributs additionnels suivants (dans la mesure où vous aviez envoyé dès le départ ces champs dans la transaction e-Commerce).

Champ	Usage
complus*	Une valeur que vous souhaitiez recevoir
(paramplus content)*	Les paramètres que vous désiriez recevoir et leurs valeurs

* Cf. Paramètres du retour d'information variable (documentation e-Commerce)

Exemple d'une réponse XML à une interrogation directe (direct query) pour une transaction e-Commerce

<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="9" amount="125" currency="EUR" PM="CreditCard" BRAND="VISA" CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55" COMPLUS="123456789123456789123456789" SessionID="126548354" ShopperID="73541312"/>

6.3 Statuts possibles de réponse

Le champ STATUS comprendra le statut de la transaction. (cf. Statuts possible).

Seul le statut ci-dessous est spécifiquement lié à la recherche (query) elle-même:

Statut	NCERROR	NCSTATUS	Explication
88			La recherche (query) sur querydirect.asp a échoué

6.4 Requête Directe comme sécurité

Les temps de réponse pour une requête de transaction DirectLink sont généralement de quelques secondes; certains acquéreurs peuvent, cependant, avoir des temps de réponse plus longs.

Si vous n'avez pas reçu une réponse de notre système après 30 secondes, vous pouvez envoyer une requête à querydirect.asp, demandant le statut de votre transaction la plus récente à orderdirect.asp. Si vous recevez une réponse immédiate contenant le statut non final pour la transaction, il se pourrait qu'il y ait des problèmes chez l'acquéreur.

Si vous n'avez pas reçu une réponse à cette interrogation directe (direct query) après 10 secondes, il se pourrait qu'il y ait des problèmes de notre côté. Vous pouvez répéter cette requête vers querydirect.asp toutes les 30 secondes jusqu'à ce que vous receviez une réponse dans les 10 secondes.

A noter que :

- Ce système de contrôle ne pourra pointer vers des problèmes de notre côté que s'il existe un contrôle de votre côté pour vérifier que les requêtes partent de vos serveurs correctement.
- Un problème de notre côté ne sera pas nécessairement toujours causé par un downtime, mais pourrait également être le résultat de temps de réponse lents liés à des problèmes de base de données par exemple.
- Veuillez utiliser ces contrôles de manière judicieuse afin d'éviter de bombarder nos serveurs avec des requêtes, sans quoi nous pourrions réduire votre accès à la page querydirect.asp.

Important

Afin de protéger notre système de surcharges non nécessaires, nous interdisons les contrôles préalables du système qui incluent l’envoi de fausses transactions ou d’interrogations (queries) systématiques, ainsi que les interrogations (queries) systématiques utilisées pour obtenir le retour d’information de transaction (transaction feedback) pour chaque transaction.

7. Demande de politique de confidentialité à l'attention du responsable du traitement des données

En vertu des articles 12, 13 et 14 du RGPD, le responsable du traitement a l'obligation d'informer ses clients finaux du futur traitement de leurs données personnelles. Il indiquera le type de données personnelles utilisées pour une transaction spécifique (méthode de paiement sélectionnée, responsable du traitement des données, acquéreur, fraude, etc.). Le résultat doit être disponible et visible au moment de la collecte des données et le titulaire de la carte doit pouvoir le télécharger et l'imprimer. Conformément au RGPD, vous devez fournir ces informations à votre client avant qu'il ne valide sa transaction. Ces informations seront de préférence affichées sur la page de saisie des données de compte ou carte bancaire.
La demande de politique de confidentialité ci-dessous vous permet de récupérer toutes les informations que vous devez indiquer à votre client sur nos services pour être en conformité avec le RGPD.

7.1 Demande de requête

7.1.1 Demande d'URL

• L'URL de demande dans l'environnement TEST est https://secure.ogone.com/ncol/test/privacy-policy.asp

• L'URL de demande dans l'environnement PRODUCTION est https://secure.ogone.com/ncol/prod/privacy-policy.asp

Remplacer « test » par « prod »

Remplacez « test » par « prod » dans l'URL de demande pour passer au compte de production.

7.1.2 Demande de Paramètres

Le tableau suivant contient les paramètres de demande obligatoires à envoyer à vos clients concernant l'utilisation de leurs informations à caractère personnel :

Champ	Format	Description
USERID	Chaîne	Votre utilisateur API
PSWD	Chaîne	Votre mode de passe utilisateur API
PSPID	Chaîne	PSPID de votre compte
BRAND	Chaîne (p. ex. Visa)	Facultatif : marque du moyen de paiement Vous pouvez envoyer ce champ plusieurs fois pour obtenir immédiatement le résultat de plusieurs marques. • L'envoi d'aucune marque revient au même que l'envoi de toutes vos marques actives. • Les marques formatées vides/incorrectes sont ignorées.
LANGUAGE	ISO 639-1 : codes à deux lettres (p. ex. FR)	Facultatif : la langue souhaitée du texte à récupérer. Si celle-ci n'est pas indiquée, le texte sera renvoyé dans la langue configurée par le commerçant.

7.1.3 Page de test

Vous pouvez tester des demandes de requête directes : https://secure.ogone.com/ncol/test/privacy-policy.asp

7.2 Réponse de requête

Ci-dessous figure la liste des éléments XML et des exemples de réponses XML obtenues pour différents résultats.

Nom	Format	Description
Response	Complexe	Root node, always present
Response.Status	Chaîne, valeurs possibles : Success, SuccessWithWarnings, Error	Toujours présent
Response.Body	Complexe	Présent uniquement quand Response.Status = Success ou SuccessWithWarnings
Response.Body.Html	Chaîne / html	Vide si Response.Status = SuccessWithWarnings & Response.Warnings.Warning.Code = NoContent
Response.Errors	Complexe	Présent uniquement quand Response.Status = Error
Response.Errors.Error	Complexe	Peut se produire plusieurs fois à l'intérieur d'un nœud <Errors>
Response.Warnings	Complexe	Uniquement présent quand Response.Status = SuccessWithWarnings ou Error
Response.Warnings.Warning	Complexe	Se produit plusieurs fois dans un nœud <Warnings>
Response.Errors.Error.Code Response.Warnings.Warning.Code	Chaîne, valeurs possibles : •À l'intérieur d'un nœud <Error> : non autorisé, InternalServerError •À l'intérieur d'un nœud <Warning> : NoContent	Toujours présent à l'intérieur d'un nœud <Error> ou <Warning>
Response.Errors.Error.Message Response.Warnings.Warning.Message	Chaîne	Facultatif

Si vous obtenez Response.Status=Error, voir Response.Errors.Error pour corriger l'erreur.
Ci-dessous figurent deux exemples de réussite :
1. Exemple de réponse XML pour un succès avec avertissements. L'exemple est affiché si aucune information à caractère personnel ne doit être divulguée au client.

```
<?xml version="1.0" encoding="utf-8"?>
 <Response>
    <Status>SuccessWithWarnings</Status>
    <Warnings>
        <Warning>
            <Code>NoContent</Code>
        </Warning>
```

```
    </Warnings>
    <Body>
        <Html/>
    </Body>
 </Response>
```

2. Exemple de réponse XML pour un succès avec contenu. L'exemple est affiché en deux sections.

```
<?xml version="1.0" encoding="utf-8"?>
<Response>
    <Status>Success</Status>
    <Body>
        <Html><![CDATA[<ul><li><h2>Title 1</h2><p>Content 1</p></li><li>
<h2>Title 2 (VISA, American Express)</h2><p>Content 2</p></li></ul>]]></Html>
    </Body>
</Response>
```

8. Exceptions parmi les moyens de paiement

Pour certains moyens de paiement, les valeurs des paramètres diffèrent des valeurs standard pour les cartes de crédit.

8.1 Direct Debits

8.1.1 Direct Debits AT

Le tableau ci-dessous contient les valeurs spécifiques des paramètres permettant la transmission de transactions Direct Debit AT via DirectLink.

Format: AN= Alphanumérique / N=Numérique, le nombre maximum de caractères autorisés

Champ	Utilisation	Format/Valeur
CARDNO	Numéro de compte bancaire	AN, 21 Format: XXXXXXXXXXXBLZYYYYY XXXXXXXXXX: numéro de compte, numérique, 11 chiffres. YYYYY: Code bancaire (Bankleitzahl), 5 chiffres.
CN	Nom du titulaire de compte bancaire	AN, 35
ED	Date d'expiration	MM/AA or MMAA
OPERATION	Code d'opération	A, 3 Valeurs possibles: • RES: autorisation • SAL/SAS: argent débité du compte bancaire • RFD/RFS: argent remboursé (*)
OWNERADDRESS	Adresse du titulaire de compte bancaire	AN, 50
OWNERTOWN	Ville du titulaire de compte bancaire	AN, 40
OWNERZIP	Code postal du titulaire de compte bancaire	AN, 10
PM	Moyen de paiement	AN, 25 “Direct Debits AT”

(*Si l’option “Remboursement” est disponible et active, et les remboursements DTAUS sont disponibles)

8.1.2 Direct Debits DE (ELV)

Le tableau suivant contient les valeurs spécifiques des paramètres permettant la transmission de transactions ELV en mode DirectLink. (à l’exception de Wirecard/Billpay)

Format: AN= Alphanumérique / N=Numérique, le nombre maximum de caractères autorisés

Champ	Usage	Format/Valeur	Obligatoire

Champ	Usage	Format/Valeur	Obligatoire
CARDNO	Numéro de compte bancaire	IBAN: 22 caractères alphanumériques OR Numéro de compte bancaire + BLZ. Format: XXXXXXXXXBLZYYYYYYYY XXXXXXXXXX: numéro de compte, numérique, 1 to 10 chiffres. YYYYYYYY: Code bancaire (Bankleitzahl), 8 chiffres.	Oui
CN	Nom du titulaire de compte bancaire	AN, 35	Non
ED	Date d'expiration	MM/AA ou MMAA	Oui
MANDATEID	Référence unique de mandat.	Telego: AN, 35 / Charset: “A-Z a-z 0-9 space /-?:().,'+”) Si non fournie, la plateforme prendra l’ORDERID ou le PAYID Easycash: Format: AN, 27 / Charset: “A-Z a-z 0-9 space /-?:().,'+”) Note: Si non fournie, easycash générera une valeur.	Non
OPERATION	Code d'opération	A, 3 Valeurs possibles: • RES: autorisation • SAL/SAS: argent débité du compte bancaire • RFD/RFS: argent remboursé (*)	Non
OWNERADDRESS	Adresse du titulaire de compte bancaire	AN, 50	Oui
OWNERTOWN	Ville du titulaire de compte bancaire	AN, 40	Oui
OWNERZIP	Code postal du titulaire de compte bancaire	AN, 10	Oui
PM	Moyen de paiement	AN, 25 "Direct Debits DE”	Oui

Note: Ces champs peuvent être retournés dans une réponse XML en mode DirectLink XML et doivent être inclus dans le calcul du SHA-IN (de manière optionnelle aussi le SHA-OUT)

(*Si la function REMBOURSEMENT est disponible et active et les Remboursements DTAUS sont disponibles)

8.1.3 Direct Debits NL

Le tableau suivant contient les valeurs spécifiques des paramètres permettant la transmission de transactions Direct Debits NL via DirectLink.

Format: AN= Alphanumérique / N=Numérique, le nombre maximum de caractères autorisés

Champ	Usage	Format/Valeur
CARDNO	Numéro de compte bancaire	Numéro de compte néerlandais classique: max. 10 caractères alphanumériques (si inférieur, pad à gauche avec des zéros). OU Numéro de compte IBAN: max. 35 caractères alphanumériques (SEPA)
CN	Nom du titulaire de compte bancaire	AN, 35
ED	Date d'expiration	MM/AA ou MMAA
OPERATION	Code d'opération	A, 3 Valeurs possibles: • SAL ou SAS: argent débité du compte bancaire • RFD ou RFS: argent remboursé (remboursement)
OWNERTOWN	Ville du titulaire de compte bancaire	AN, 40
PM	Moyen de paiement	AN, 25 “Direct Debits NL”
Seulement pertinent pour les transactions SEPA (*):		
BIC	Code d’Identification de la Banque.	AN, 11
MANDATEID	Référence unique de mandat. Note: Si non fournie, l’ORDERID sera pris à la place.	AN, 35 Pas d’espace; ne peut commencer ni finir par une barre oblique "/" ou contenir deux barres obliques (slashes) consécutives.
SEQUENCETYPE	Type de transaction Direct Debit Note: Si non fournie, la transaction sera considérée comme “seule et unique” (“one-off") (OOFF sera appliqué).	Valeurs possible pour indiquer le type de transaction Direct Debit (AN, 4): • "FRST": Première collecte d’une série d’instructions pour Direct Debit • "RCUR": Instructions pour Direct Debit où l’autorisation du débiteur est utilisée pour des transactions classiques en Direct Debit initiées par le créditeur • "FNAL": Dernière collecte d’une série d’instructions pour Direct Debit (par après, le même MandateID ne peut plus

Champ	Usage	Format/Valeur
		être utilisé) • "OOFF": Instruction pour Direct Debit où l'autorisation du débiteur est utilisée pour initier une seule transaction Direct Debit
SIGNDATE	La date de mandat a été signée par l'acheteur. Note: Si non fournie, la date de transaction sera prise à la place.	AAAAMMJJ

(*SEPA: Single Euro Payments Area)

Note: Ces champs peuvent être retournés dans une réponse XML en mode DirectLink XML et doivent être inclus dans le calcul du SHA-IN (de manière optionnelle aussi le SHA-OUT).

8.2 Moyen de paiement où seule la maintenance est possible via DirectLink

Pour certains moyens de paiement (hors cartes de crédit), vous ne pouvez pas envoyer de nouvelles transactions via DirectLink, mais vous pouvez envoyer des opérations de maintenance via DirectLink. C'est par exemple le cas pour PostFinance Card, PostFinance e-finance, PayPal Express Checkout et TUNZ. Lorsque vous envoyez des opérations de maintenance, PM/BRAND/CARDNO/ED ne sont pas des données requises, aucune valeur spécifique ne doit donc être envoyée pour ces moyens de paiement.