SOLUTION COLLECT

Paiements par token et abonnements

Guide d'implémentation

Version du document 3.16.3

Sommaire

1. PRÉSENTATION DU SERVICE 4

2. LE PARTAGE D'ALIAS 5

3. MOYENS DE PAIEMENT COMPATIBLES 6

4. CHAÎNAGE DES TRANSACTIONS CIT/MIT 12

5. CAS D'UTILISATION 13

5.1. Création de l'alias sans paiement 14

5.2. Modification des informations associées à l'alias 16

5.3. Création de l'alias lors d'un paiement 18

5.4. Création de l'alias lors de la souscription à un abonnement 20

5.5. Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement 23

5.6. Paiement par alias 26

5.7. Utilisation d'un alias pour souscrire à un abonnement 28

5.8. Paiement avec proposition au porteur de créer un alias 30

6. CYCLE DE VIE D'UN PAIEMENT RÉCURRENT 32

6.1. Liste des codes retour de la demande d'autorisation 32

6.2. Notification par e-mail en cas de refus d'une échéance 35

7. PROPOSER DES TENTATIVES DE PAIEMENT SUPPLÉMENTAIRES 36

8. ÉTABLIR LE DIALOGUE AVEC LA PLATEFORME DE PAIEMENT 37

8.1. Similarités avec le paiement unitaire 37

9. CONFIGURER LES NOTIFICATIONS 38

9.1. Configurer la notification à la fin du paiement 39

9.2. Configurer la notification en cas d'abandon ou annulation 40

9.3. Configurer la notification sur une opération provenant du Back Office 41

9.4. Configurer la notification à la création d'un abonnement 42

9.5. Configurer la notification sur autorisation par batch 43

9.6. Rejeu automatique en cas d'échec 44

9.7. Configurer les e-mails envoyés à l'acheteur 46

10. GÉNÉRER UN FORMULAIRE DE PAIEMENT 47

10.1. Créer un formulaire 'Création de l'alias sans paiement' 49

10.2. Créer un formulaire 'Modification des informations associées à l'alias' 49

10.3. Créer un formulaire 'Création de l'alias lors d'un paiement' 51

10.4. Créer un formulaire 'Création de l'alias lors de la souscription à un abonnement' 53

10.5. Créer un formulaire 'Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement' 55

10.6. Créer un formulaire 'Paiement par alias'.... 58
10.7. Créer un formulaire 'Utilisation d'un alias pour souscrire à un abonnement'.... 60
10.8. Créer un formulaire 'Paiement avec proposition au porteur de créer un alias'.... 62

11. UTILISER DES FONCTIONS COMPLÉMENTAIRES.... 64
11.1. Définir un montant différent pour les n premières échéances.... 65
11.2. Définir la devise pour la création ou la mise à jour d'un alias.... 66

12. CALCULER LA SIGNATURE.... 67

13. ENVOYER LA DEMANDE DE PAIEMENT.... 69
13.1. Rediriger l'acheteur vers la page de paiement.... 69
13.2. Gérer les erreurs.... 69

14. IMPLÉMENTER L'IPN.... 72
14.1. Préparer son environnement.... 73
14.2. Récupérer les données retournées dans la réponse.... 74
14.3. Calculer la signature de l'IPN.... 75
14.4. Comparer les signatures.... 76
14.5. Analyser la nature de la notification.... 77
14.6. Traiter les données de la réponse.... 78
14.6.1. Création d'un alias sans paiement.... 78
14.6.2. Modification des informations associées à l'alias.... 83
14.6.3. Création de l'alias lors d'un paiement.... 87
14.6.4. Création de l'alias lors de la souscription à un abonnement.... 92
14.6.5. Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement.... 97
14.6.6. Paiement par alias.... 102
14.6.7. Souscription à un abonnement.... 106
14.6.8. Paiement avec proposition au porteur de créer un alias.... 109
14.6.9. Paiement d'une échéance d'un abonnement.... 113
14.7. Test et troubleshooting.... 117

15. OBTENIR DE L'AIDE.... 120

16. ANNEXES.... 121
16.1. Créer automatiquement un abonnement par Web Services.... 121
16.2. Résilier automatiquement un abonnement par Web services.... 121
16.3. Cartes de test.... 121

1. PRÉSENTATION DU SERVICE

Gestion des paiements par alias

Le service permet d'associer un alias à un moyen de paiement pour faciliter les paiements ultérieurs.

Avantages :

- Effectuer des paiements rapides et sécurisés.

  L'acheteur n'a plus à saisir ses données bancaires ou son IBAN (paiement en 1 clic).

  La plateforme stocke données bancaires conformément aux exigences PCI-DSS. Seul l'alias transite lors des échanges.
- Effectuer des paiements par abonnement.
- Identifier les cartes en fin de validité.

  La plateforme vous alerte sur les alias dont la carte arrive à échéance.
- Mettre à jour les données bancaires associées à un alias depuis la page de paiement ou depuis le Back Office Expert.
- Détecter automatiquement un moyen de paiement expiré et proposer sa mise à jour lors d'un paiement par alias.
- Détecter lors de la création d'un alias, si le moyen de paiement a déjà été enregistré précédemment.
- Modifier les données de l'acheteur.

Les alias sont utilisables par toutes les boutiques d'une même société.

Durée de conservation :

- En respect des règles de sécurité et de protection des données bancaires exigées par PCI DSS, les données du moyen de paiement sont purgées au delà de 15 mois de non utilisation de l'alias associé.
- La plateforme purge toutes les cartes expirées depuis plus d'un an et tous les alias non utilisés depuis plus de 2 ans.

Gestion des paiements par abonnement

Le service permet aux marchands de créer des abonnements avec montants et échéances fixes avec ou sans date de fin, dans la limite de la validité de la carte.

Fonctionnement :

- Lors de la création de l'abonnement, le marchand définit la date de début, le montant des échéances et la règle de récurrence à appliquer.
- Une fois la date d'effet atteinte, la plateforme de paiement procède automatiquement au traitement des échéances.
- Le marchand n'a alors plus la possibilité de modifier le montant des échéances.

Pour recevoir une notification, la règle "URL de notification à la création d'un abonnement" doit être activée et configurée depuis le Back Office Expert (menu **Paramétrage** > **Règles de notifications**).

En mode test, la transaction de la première échéance est créée au plus tard une heure après l'abonnement, selon l'échéancier déterminé par la règle de l'abonnement.

En mode production, les transactions sont créées une fois par jour entre 00:00 et 05:00 UTC.

Tous droits réservés

2. LE PARTAGE D'ALIAS

Par défaut, les alias sont utilisables par toutes les boutiques d'une même société.

La plateforme de paiement permet le partage des alias (token) entre plusieurs sociétés.

Chaque alias de chaque société doit être unique et associé à une carte bancaire. Toutes les alias doivent être impérativement générés par la plateforme de paiement.

Le partage d'alias entre plusieurs sociétés ne fonctionne pas avec les alias associés à un mandat SEPA.

L'activation de cette fonctionnalité n'est pas gratuite. Contactez votre interlocuteur commercial chez Lyra Collect.

Tous droits réservés

3. MOYENS DE PAIEMENT COMPATIBLES

Liste des moyens de paiement compatibles avec le service de Gestion des paiements par alias:

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement par alias
ACCORD	Carte Cadeau Illicado	ILLICADO	✗
ACCORD	Carte enseigne Accord	ACCORD_STORE	✗
ACCORD_SANDBOX	Carte Cadeau Illicado - Mode sandbox	ILLICADO_SB	✗
ALIPAY_PLUS	Akulaku PayLater ID	AKULAKU_ID	✗
ALIPAY_PLUS	Akulaku PayLater PH	AKULAKU_PH	✗
ALIPAY_PLUS	Alipay CN (Chine)	ALIPAY_CN	✗
ALIPAY_PLUS	Alipay HK (Hong Kong)	ALIPAY_HK	✗
ALIPAY_PLUS	BillEase	BILLEASE	✗
ALIPAY_PLUS	Boost	BOOST	✗
ALIPAY_PLUS	BPI	BPI	✗
ALIPAY_PLUS	Dana	DANA	✗
ALIPAY_PLUS	GCash	GCASH	✗
ALIPAY_PLUS	Kakao Pay	KAKAOPAY	✗
ALIPAY_PLUS	Krevido	KREDIVO_ID	✗
ALIPAY_PLUS	Maya	MAYA	✗
ALIPAY_PLUS	MPay	MPAY	✗
ALIPAY_PLUS	Rabbit LINE Pay	RABBIT_LINE_PAY	✗
ALIPAY_PLUS	Touch 'n Go eWallet	TNG	✗
ALIPAY_PLUS	Toss Pay	TOSS	✗
ALIPAY_PLUS	TrueMoney Wallet	TRUEMONEY	✗
ALMA	Alma en 2 fois	ALMA_2X	✗
ALMA	Alma en 2 fois	ALMA_2X	✗
ALMA	Alma en 3 fois	ALMA_3X	✗
ALMA	Alma en 4 fois	ALMA_4X	✗
ALMA	Alma en 10 fois	ALMA_10X	✗
ALMA	Alma en 12 fois	ALMA_12X	✗

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement par alias
AMEXGLOBAL	American Express	AMEX	✅
APPLE PAY	Paiement par Wallet Apple Pay	APPLE_PAY	❌
AURORE	Carte Cpay	AURORE-MULTI	❌
CB	Carte bancaire CB	CB	✅
CB	Maestro	MAESTRO	❌
CB	Mastercard	MASTERCARD	✅
CB	Carte Titre-Restaurant Apetiz	APETIZ	✅
CB	Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	✅
CB	Carte Titre-Restaurant Mastercard 1ère génération	EDENRED	✅
CB	Carte Titre-Restaurant Sodexo	SODEXO	✅
CB	Carte virtuelle e-Carte Bleue	E-CARTEBLEUE	✅
CB	Visa	VISA	✅
CB	Visa Electron	VISA_ELECTRON	✅
CB	Visa Vpay	VPAY	✅
CONECS	Carte Titre-Restaurant Apetiz	APETIZ	✅
CONECS	Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	✅
CONECS	Carte Titre-Restaurant Conecs	CONECS	✅
CONECS	Carte Titre-Restaurant Sodexo	SODEXO	✅
COFIDIS	Cofidis en 3 fois (France)	COFIDIS_3X_FR	❌
COFIDIS	Cofidis en 4 fois (France)	COFIDIS_4X_FR	❌
COFIDIS	Cofidis en 5 ou 12 fois (France)	COFIDIS_LOAN_CB	❌
COFIDIS	Cofidis Pay (France)	COFIDIS_PAY_FR	❌
COFIDIS	Cofidis en 10 ou 60 fois (France)	COFIDIS_LOAN_FR	❌
COFIDIS	Cofidis Pay Later (France)	COFIDIS_DFPAY_FR	❌

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement par alias
COFIDIS	Cofidis en 4 fois (Espagne)	COFIDIS_4X_ES	✗
COFIDIS	Cofidis en 5 ou 12 fois (Espagne)	COFIDIS_LOAN_ES	✗
CVCONNECT	Chèque-Vacances Connect	CVCO	✗
EDENRED	Ticket Eco Chèque Edenred	EDENRED_EC	✓
EDENRED	Ticket Sport & Culture Edenred	EDENRED_SC	✓
EDENRED	Ticket Compliment Edenred	EDENRED_TC	✓
EDENRED	Ticket Restaurant Edenred	EDENRED_TR	✓
FLOA	Floa en 3 fois	FLOA_3X	✗
FLOA	Floa en 4 fois	FLOA_4X	✗
FLOA	Floa en 10 fois	FLOA_10X	✗
FLOA	Floa Pay Later	FLOA_PAYLATER	✗
FRANFINANCE	Paiement en 3 fois Franfinance	FRANFINANCE_3X	✗
FRANFINANCE	Paiement en 4 fois Franfinance	FRANFINANCE_4X	✗
FRANFINANCE_SB	Paiement en 3 fois Franfinance - Mode sandbox	FRANFINANCE_3X	✗
FRANFINANCE_SB	Paiement en 4 fois Franfinance - Mode sandbox	FRANFINANCE_4X	✗
FULLCB	Paiement en 3x sans frais par BNPP PF	FULLCB3X	✗
FULLCB	Paiement en 4x sans frais par BNPP PF	FULLCB4X	✗
GATECONEX	Bancontact	BANCONTACT	✗
GATECONEX	Diners Club	DINERS	✓
GATECONEX	Discover	DISCOVER	✓
GATECONEX	Carte virtuelle e-Carte Bleue	E-CARTEBLEUE	✓
GATECONEX	Maestro	MAESTRO	✗
GATECONEX	Mastercard	MASTERCARD	✓
GATECONEX	Visa	VISA	✓

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement par alias
GATECONEX	Visa Electron	VISA_ELECTRON	✗
GATECONEX	Visa Vpay	VPAY	✗
GICC	Bancontact	BANCONTACT	✗
GICC	Maestro	MAESTRO	✗
GICC	Mastercard	MASTERCARD	✓
GICC	Visa	VISA	✓
GICC	Visa Electron	VISA_ELECTRON	✗
GICC_DINERS	Diners Club	DINERS	✓
GICC_DINERS	Discover	DISCOVER	✓
GICC_MAESTRO	Bancontact	BANCONTACT	✗
GICC_MAESTRO	Maestro	MAESTRO	✗
GICC_MASTERCARD	Mastercard	MASTERCARD	✓
GICC_VISA	Visa	VISA	✓
GICC_VISA	Visa	VPAY	✗
GICC_VISA	Visa Electron	VISA_ELECTRON	✗
GOOGLEPAY	Paiement par Wallet Google Pay	GOOGLEPAY	✗
JCB	JCB	JCB	✓
LYRA_COLLECT_PPRO	Paiement par Wallet Alipay	ALIPAY	✗
LYRA_COLLECT_PPRO	Bancontact	BANCONTACT	✗
LYRA_COLLECT_PPRO	Virement bancaire iDEAL	IDEAL	✗
LYRA_COLLECT_PPRO	Paiement par coupon sur le réseau MultiBanco	MULTIBANCO	✗
LYRA_COLLECT_PPRO	Virement bancaire MyBank	MYBANK	✗
LYRA_COLLECT_PPRO	Virement bancaire Przelewy24	PRZELEWY24	✗
LYRA_COLLECT_PPRO	Carte UnionPay	UNION_PAY	✗
LYRA_COLLECT_PPRO	Paiement par wallet We Chat Pay	WECHAT	✗
MULTIBANCO	MB Reference	MULTIBANCO	✗
MULTIBANCO	MB Way	MB_WAY	✗

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement par alias
ONEY	Paiement en 3 ou 4 fois par carte bancaire FacilyPay	ONEY	✗
ONEY_API	Paiement 3x 4x Oney	ONEY_3X_4X	✗
ONEY_API	Paiement 10x 12x Oney	ONEY_10X_12X	✗
ONEY_API	Paiement Oney Pay Later	ONEY_PAYLATER	✗
ONEY_API	Cartes Enseignes partenaires d'Oney.	ONEY_ENSEIGNE	✗
ONEY_API_SANDBOX	Paiement 3x 4x Oney en mode sandbox	ONEY_3X_4X	✗
ONEY_API_SANDBOX	Paiement 10x 12x Oney en mode sandbox	ONEY_10X_12X	✗
ONEY_API_SANDBOX	Paiement Oney Pay Later en mode sandbox	ONEY_PAYLATER	✗
ONEY_API_SANDBOX	Cartes Enseignes partenaires d'Oney en mode sandbox.	ONEY_ENSEIGNE	✗
ONEY_API_SB	Paiement en 3 ou 4 fois Oney - Mode sandbox	ONEY_3X_4X	✗
ONEY_SANDBOX	Paiement en 3 ou 4 fois par carte bancaire FacilyPay - Mode Sandbox	ONEY_SANDBOX	✗
PAYDIREKT_V2	Virement bancaire paydirekt	PAYDIREKT	✗
PAYPAL	Paiement par PayPal	PAYPAL	✓
PAYPAL_SB	Paiement par PayPal - Mode sandbox	PAYPAL_SB	✓
PAYPAL_BNPL	Paiement par PayPal Pay Later	PAYPAL_BNPL	✓
PAYPAL_BNPL_SB	Paiement par PayPal Pay Later - Mode sandbox	PAYPAL_BNPL_SB	✓
PLANET_DCC	Mastercard	MASTERCARD	✓
PLANET_DCC	Visa	VISA	✓
POSTFINANCEV2	Paiement par carte PostFinance Card	POSTFINANCE	✗
POSTFINANCEV2	Virement bancaire PostFinance Efinance	POSTFINANCE_EFIN	✗
REDSYS_REST	American Express	AMEX	✓
REDSYS_REST	Diners Club	DINERS	✓
REDSYS_REST	JCB	JCB	✓

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement par alias
REDSYS_REST	Maestro	MAESTRO	✅
REDSYS_REST	Mastercard	MASTERCARD	✅
REDSYS_REST	Visa	VISA	✅
REDSYS_REST	Visa Electron	VISA_ELECTRON	✅
REDSYS	Visa Vpay	VPAY	✅
SAMSUNG PAY	Paiement par Wallet Samsung Pay	SAMSUNG_PAY	❌
SEPA	Prélèvement Bancaire SEPA DIRECT DEBIT	SDD	✅

Tous droits réservés

4. CHAÎNAGE DES TRANSACTIONS CIT/MIT

La deuxième directive sur les services de paiement (DSP2) impose l'authentification du porteur de carte pour toute transaction e-commerce initiée par celui-ci.

Il faut identifier si la demande de paiement est initiée :

- **CIT (Customer Initiated Transaction)** : Transaction initiée par l'acheteur avec interaction.

  Exemple : Paiement ou enregistrement d'une carte nécessitant la saisie des données.

- **MIT (Merchant Initiated Transaction)** : Transaction initiée par le marchand, sans la présence de l'acheteur, liée à une transaction CIT.

  Exemple : Échéance d'un paiement en plusieurs fois.

Chaînage des opérations :.

Pour une transaction **CIT**, la réglementation impose l'authentification du porteur. Après la demande d'autorisation ou de renseignement, l'émetteur retourne un identifiant unique, appelé "référence de chaînage". Cette référence est utilisée pour les transactions MIT afin de signaler à l'émetteur que la transaction fait partie d'une série de paiement, pour laquelle le porteur s'est authentifié lors du premier paiement.

Sans cette référence, l'émetteur peut refuser une transaction MIT pour défaut d'authentification (soft decline).

Tous droits réservés

5. CAS D'UTILISATION

Le formulaire de paiement permet de réaliser les opérations suivantes classées par cas.

Chacun de ces cas correspond à une valorisation différente du champ **vads_page_action**.

Cas d'usage	Valorisation du champ vads_page_action
Création de l'alias sans paiement	REGISTER
Mise à jour des informations associées à l'alias	REGISTER_UPDATE
Création de l'alias lors d'un paiement	REGISTER_PAY
Création de l'alias lors de la souscription à un abonnement	REGISTER_SUBSCRIBE
Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement	REGISTER_ PAY_SUBSCRIBE
Paiement par alias	PAYMENT
Utilisation d'un alias pour souscrire à un abonnement	SUBSCRIBE
Paiement avec proposition au porteur de créer un alias	ASK_ REGISTER_PAY

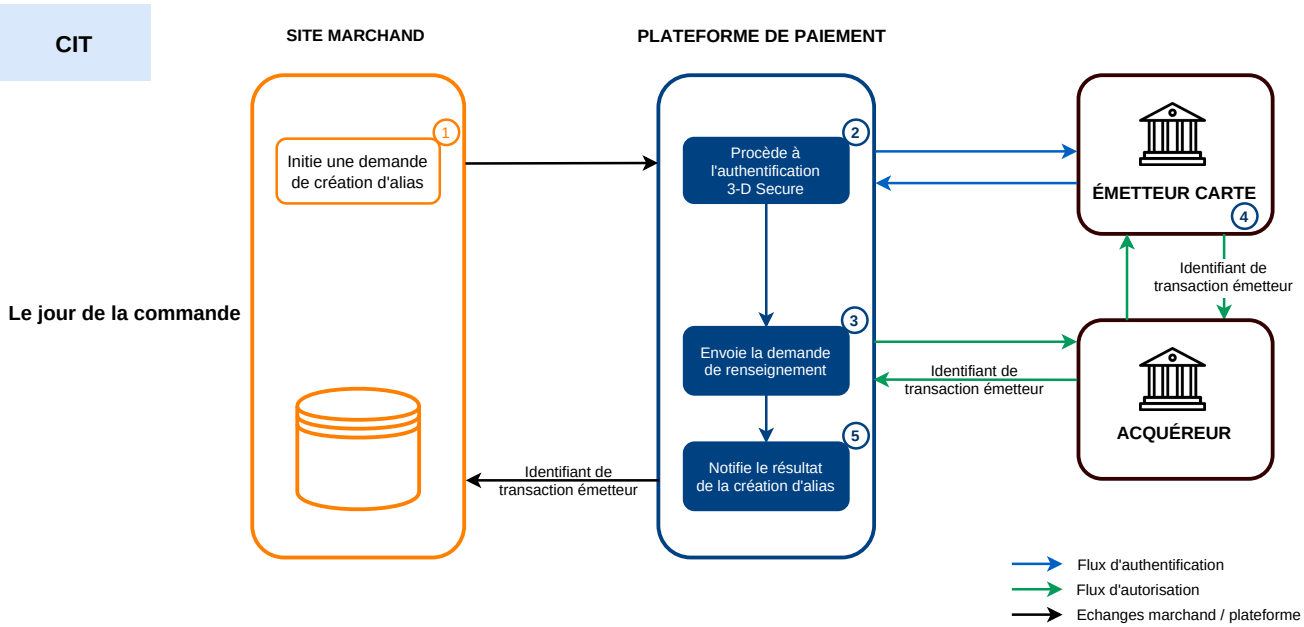
Selon le cas d'utilisation (valorisation du champ **vads_page_action**), les interactions entre l'acheteur et la page de paiement seront différentes.

Tous droits réservés

5.1. Création de l'alias sans paiement

Ce cas correspond à la simple création d'un alias.

Schéma simplifié



1. Le site marchand soumet une demande de création d'alias.

   Note concernant les boutiques disposant de l'option "Conversion de devise" :

   La devise est obligatoire lors de la création d'un alias.

   Seuls les contrats supportant la devise passée en paramètre seront sélectionnés. La conversion de devise n'est donc pas prise en compte.

   Ex: Pour une demande de création d'alias en devise USD, sur une boutique associée à un contrat AMEX et un contrat CB :

   si le contrat AMEX ne supporte que la devise USD et le contrat CB ne supporte que la devise EUR, alors seules les cartes AMEX seront acceptées pour la création de l'alias.

   L'acheteur sélectionne le moyen de paiement à enregistrer, renseigne les données de son moyen de paiement puis valide.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   La réglementation impose une authentification forte pour ce cas d'usage.

   L'authentification est réalisée sur un montant de 0 EUR.

3. Une fois l'authentification terminée, la plateforme procède à la demande de renseignement en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande de renseignement.
5. La plateforme de paiement notifie le site marchand du résultat.

   La réponse contient notamment :

   - l'identifiant unique de transaction généré par l'émetteur, à titre d'information,
   - l'alias nouvellement créé.

Tous droits réservés

Cette opération donne lieu à la création d'une transaction de type VERIFICATION, visible dans le Back Office Expert et possédant les caractéristiques suivantes :

- son montant est de 1.00 EUR ou 0 EUR si l'acquéreur le supporte,
- son statut est soit "Accepté" soit "Refusé",
- elle n'est jamais remise en banque et reste dans l'onglet "Transactions en cours".

L'alias (token) ne sera pas créé si la demande d'autorisation ou de renseignement est refusée.

La plateforme affiche le ticket à l'acheteur. Il contient notamment :

- l'alias nouvellement créé,
- les données de l'acheteur.

Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail :

- la confirmation de l'enregistrement de ses informations bancaires sur la plateforme de paiement de la boutique,
- son alias (token) qu'il pourra utiliser ultérieurement pour effectuer une autre opération bancaire.

L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias.

En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) la plateforme utilisera par défaut l'identifiant de transaction émetteur comme référence de chaînage si nécessaire.

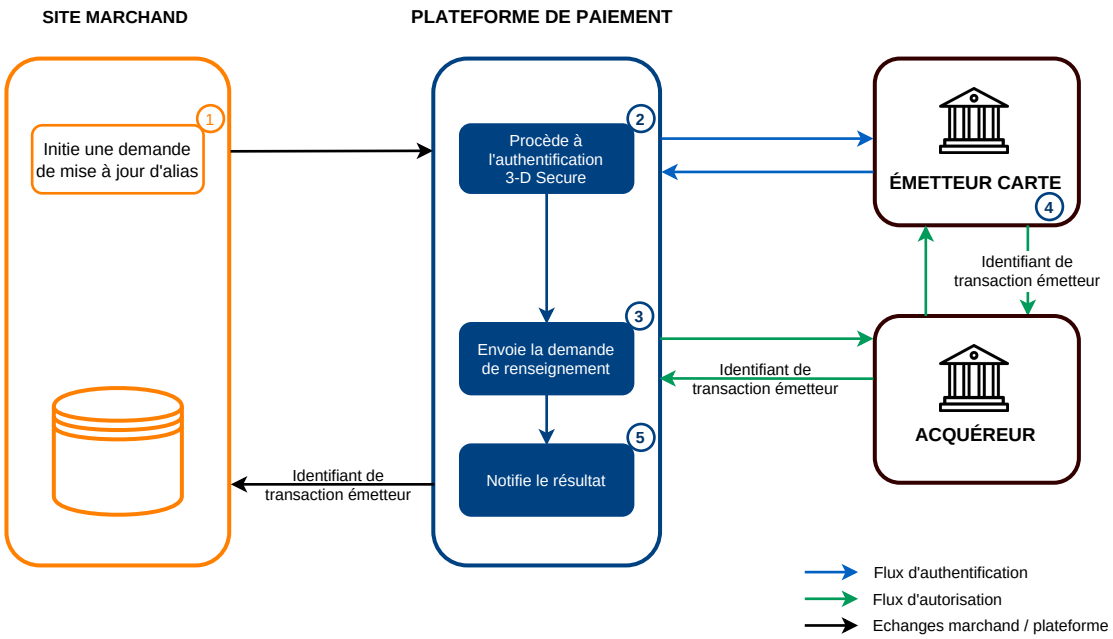
Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

5.2. Modification des informations associées à l'alias

Ce cas correspond à la mise à jour, à l'initiative de l'acheteur, des informations liées à son moyen de paiement et/ou ses informations personnelles.

Schéma simplifié

CIT



1. Le site marchand soumet une demande de mise à jour d'alias.

   L'acheteur sélectionne le moyen de paiement à enregistrer, renseigne les données de son moyen de paiement puis valide.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   > La réglementation impose une authentification forte à chaque enregistrement de carte.
   >
   > L'authentification est réalisée sur un montant de 0 EUR.

3. Une fois l'authentification terminée, la plateforme procède à la demande de renseignement en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande de renseignement.
5. La plateforme de paiement notifie le site marchand du résultat.

   La réponse contient notamment :

   - l'identifiant unique de transaction généré par l'émetteur, à titre d'information,
   - l'alias mis à jour.

   > Cette opération donne lieu à la création d'une transaction de type VERIFICATION, visible dans le Back Office Expert et possédant les caractéristiques suivantes :
   >
   > - son montant est de 1.00 EUR ou 0 EUR si l'acquéreur le supporte,
   > - son statut est soit "Accepté" soit "Refusé",
   > - elle n'est jamais remise en banque et reste dans l'onglet "Transactions en cours".

L'alias (token) ne sera pas mis à jour si la demande d'autorisation ou de renseignement est refusée.

La plateforme affiche le ticket à l'acheteur. Il contient notamment :

- l'alias,
- les données de l'acheteur.

Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail :

- la confirmation de l'enregistrement de ses informations bancaires sur la plateforme de paiement de la boutique,
- son alias (token) qu'il pourra utiliser ultérieurement pour effectuer une autre opération bancaire.

L'identifiant de transaction émetteur stocké au niveau de l'alias est remplacé par l'identifiant généré par l'émetteur lors de la mise à jour de l'alias.

En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) l'identifiant de transaction émetteur sera utilisé comme référence de chaînage si nécessaire.

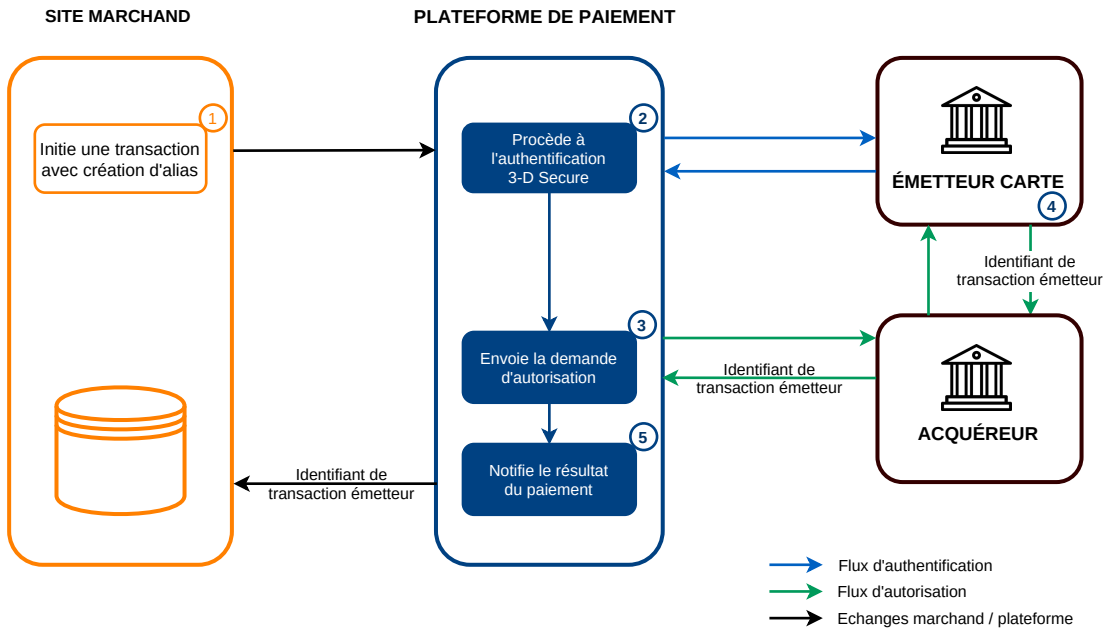
Comme pour la création d'un alias, la gestion de la référence de chaînage est transparente pour le marchand.

5.3. Création de l'alias lors d'un paiement

Dans ce cas, les paramètres nécessaires à l'inscription sont complétés par des paramètres nécessaires à une demande de paiement.

Schéma simplifié

CIT



1. Le site marchand soumet une demande de paiement avec création d'alias.

   Note concernant les boutiques disposant de l'option "Conversion de devise"

   Dès lors qu'un paiement est réalisé au moment de la commande, la conversion de devise est autorisée.

   La conversion de devise est donc supportée pour cette opération, contrairement à la création d'un alias avec ou sans abonnement.

   L'acheteur sélectionne le moyen de paiement à enregistrer, renseigne les données de son moyen de paiement puis valide.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   La réglementation impose une authentification forte pour ce cas d'usage.

   L'authentification est réalisée sur le montant du paiement.

3. Une fois l'authentification terminée, la plateforme procède à la demande d'autorisation en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande d'autorisation.
5. La plateforme de paiement notifie le site marchand du résultat.

   La réponse contient notamment :

   - le résultat du paiement,
   - l'identifiant unique de transaction généré par l'émetteur, à titre d'information,
   - l'alias nouvellement créé.

Tous droits réservés

L'alias (token) ne sera pas créé si la demande d'autorisation ou de renseignement est refusée.

La plateforme affiche le ticket à l'acheteur. Il contient notamment :

- le résultat du paiement,
- l'alias nouvellement créé.

Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail :

- le ticket de paiement
- la confirmation de l'enregistrement de ses informations bancaires sur la plateforme de paiement de la boutique,
- son alias (token) qu'il pourra utiliser ultérieurement pour effectuer une autre opération bancaire.

L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias et de la transaction.

En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) la plateforme utilisera par défaut l'identifiant de transaction émetteur comme référence de chaînage si nécessaire.

Dans le cas où le marchand duplique (**MIT**) la transaction créée le jour de la commande, la plateforme utilise automatiquement cet identifiant comme référence de chaînage.

Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

5.4. Création de l'alias lors de la souscription à un abonnement

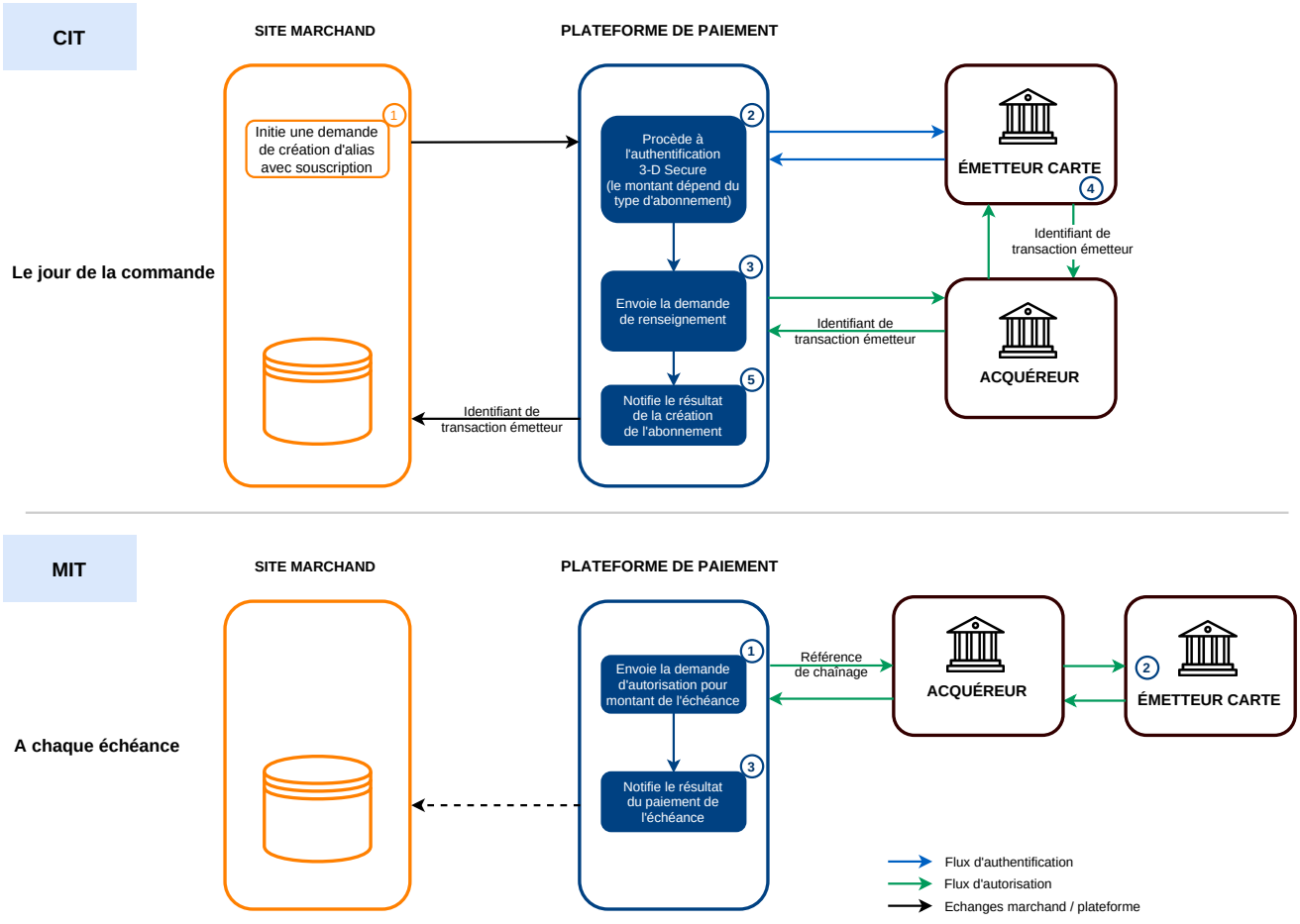
En plus des informations utilisées dans le cas de la **Création de l'alias sans paiement**, ce cas d'utilisation doit également faire apparaître des informations liées à l'abonnement telles que :

- le montant initial de l'abonnement (montant utilisé lors de la ou des premières échéances) si celui-ci est différent (optionnel),
- le montant de l'abonnement (montant des échéances ou bien celui utilisé pour les échéances suivantes lorsque la première est différente).

Aucun paiement ne sera réalisé lors de la souscription. Seule une demande de renseignement sera réalisée afin de valider les données du moyen de paiement.

Le premier paiement sera réalisé une fois la date d'effet atteinte, entre 00h00 et 05h00.

Schéma simplifié



Le jour de la commande :

1. Le site marchand soumet une demande de création d'alias et de souscription à un abonnement.

Note concernant les boutiques disposant de l'option "Conversion de devise" :

La devise est obligatoire lors de la création d'un alias.

Seuls les contrats supportant la devise passée en paramètre seront sélectionnés. La conversion de devise n'est donc pas prise en compte.

Tous droits réservés

Ex : Pour une demande de création d'alias en devise USD, sur boutique associée à un contrat AMEX et un contrat CB :

si le contrat AMEX ne supporte que la devise USD et le contrat CB ne supporte que la devise EUR, alors seules les cartes AMEX seront acceptées pour la création de l'alias.

L'acheteur sélectionne le moyen de paiement qu'il souhaite enregistrer, renseigne les données de son moyen de paiement puis valide.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   - La réglementation impose une authentification forte pour ce cas d'usage.
   - L'authentification est réalisée sur le montant de la première échéance.

3. Une fois l'authentification terminée, la plateforme procède à la demande de renseignement en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande de renseignement.
5. La plateforme de paiement notifie le site marchand du résultat.

   La réponse contient notamment :

   - l'identifiant unique de transaction généré par l'émetteur, à titre d'information,
   - l'alias nouvellement créé,
   - le détail de l'abonnement.

   Cette opération donne lieu à la création d'une transaction de type VERIFICATION, visible dans le Back Office Expert et possédant les caractéristiques suivantes :

   - son montant est de 1.00 EUR ou 0 EUR si l'acquéreur le supporte,
   - son statut est soit "Accepté" soit "Refusé",
   - elle n'est jamais remise en banque et reste dans l'onglet "Transactions en cours".

   L'alias (token) ne sera pas créé si la demande d'autorisation ou de renseignement est refusée.

   La plateforme affiche le ticket à l'acheteur. Il contient notamment :

   - l'alias nouvellement créé,
   - les montants de l'abonnement.

   Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail :

   - la confirmation de l'enregistrement de ses informations bancaires sur la plateforme de paiement de la boutique,
   - la confirmation de l'enregistrement de l'abonnement.

L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias.

En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) la plateforme utilisera par défaut l'identifiant de transaction émetteur comme référence de chaînage si nécessaire.

A chaque échéance :

1. La plateforme de paiement réalise une demande d'autorisation pour le montant de l'échéance, en fournissant l'identifiant de transaction initiale (CIT) comme référence de chaînage.

2. L'émetteur reconnaît la transaction comme une **MIT** faisant partie d'une série de paiements pour laquelle le porteur s'est authentifié préalablement et procède à la demande d'autorisation.

   La transaction ne sera pas refusée pour défaut d'authentification (soft decline).

3. Si le marchand a activé la règle de notification **URL de notification à la création d'un abonnement**, la plateforme de paiement notifie le site marchand du résultat du paiement.

Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

Tous droits réservés

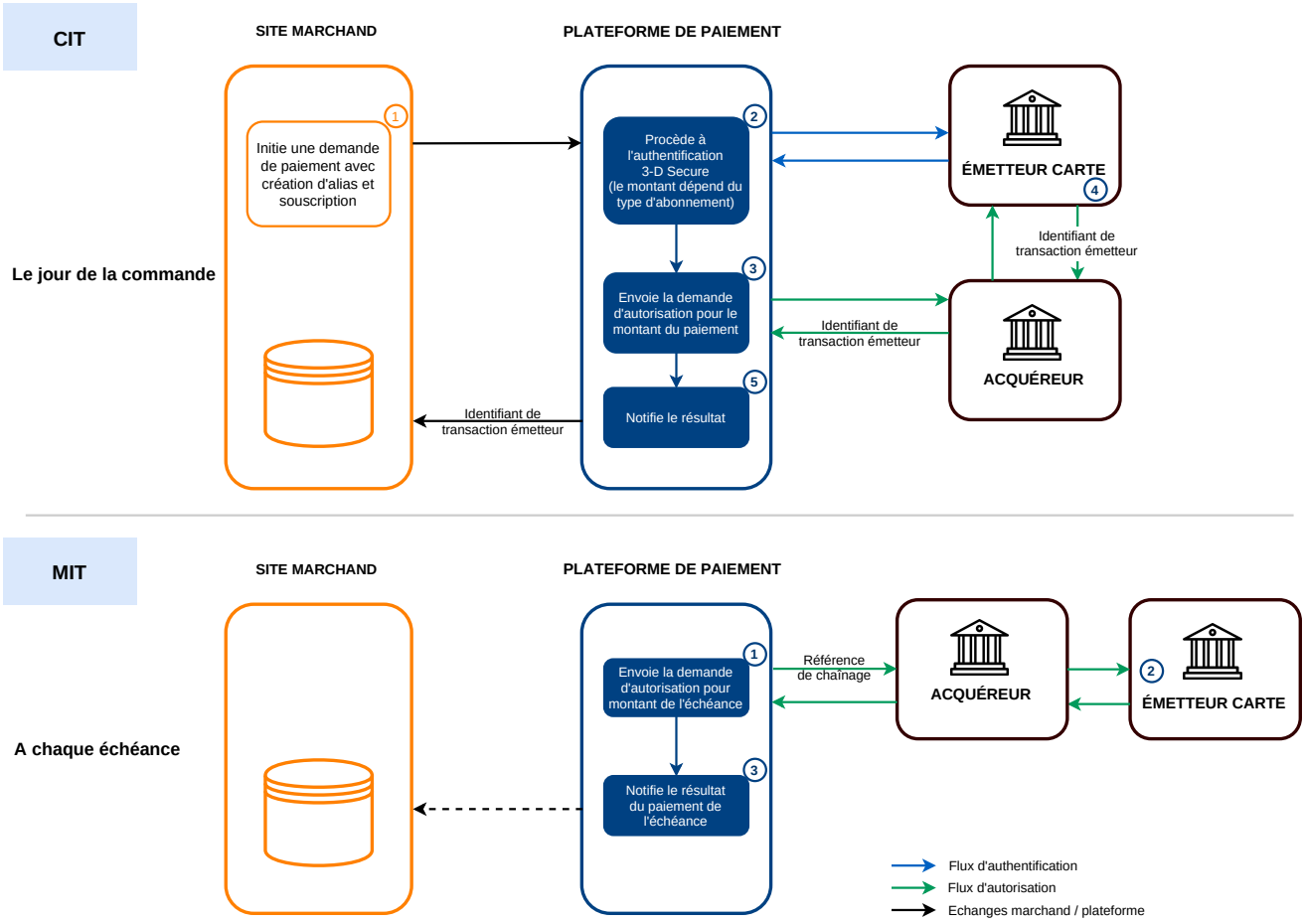
5.5. Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement

Ce cas d'utilisation doit faire apparaître des informations telles que :

- les informations sur l'acheteur,
- l'identifiant de la transaction,
- les informations sur l'abonnement (montants).

Exemple d'utilisation : un abonnement d'un montant de X EUR/ sur N mois avec frais de mise en service à payer à la prise de commande.

Schéma simplifié



Le jour de la commande :

1. Le site marchand soumet une demande de création d'alias et de souscription à un abonnement avec paiement immédiat.

   > **Note concernant les boutiques disposant de l'option "Conversion de devise"**
   >
   > Dès lors qu'un paiement est réalisé au moment de la commande, la conversion de devise est autorisée.
   >
   > La conversion de devise est donc supportée pour cette opération, contrairement à la création d'un alias avec ou sans abonnement.

   L'acheteur sélectionne le moyen de paiement à enregistrer, renseigne les données de son moyen de paiement puis valide.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

Tous droits réservés

- La réglementation impose une authentification forte pour ce cas d'usage.
- L'authentification est réalisée sur le montant de la première échéance.

3. Une fois l'authentification terminée, la plateforme procède à la demande d'autorisation en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande d'autorisation.
5. La plateforme de paiement notifie le site marchand du résultat.

   La réponse contient notamment :

   - le résultat du paiement,
   - le détail de l'abonnement,
   - l'identifiant unique de transaction généré par l'émetteur, à titre d'information,
   - l'alias nouvellement créé.

   L'alias (token) et l'abonnement ne seront pas créés si la demande d'autorisation est refusée.

   La plateforme affiche le ticket à l'acheteur. Il contient notamment :

   - le résultat du paiement,
   - les montants de l'abonnement,
   - l'alias nouvellement créé.

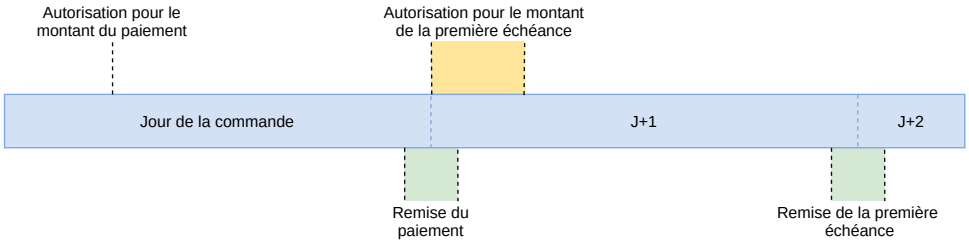
   Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail :

   - le ticket de paiement,
   - la confirmation de l'enregistrement de ses informations bancaires sur la plateforme de paiement de la boutique,
   - la confirmation de l'enregistrement de l'abonnement,
   - son alias (token) qu'il pourra utiliser ultérieurement pour effectuer une autre opération bancaire.

L'acheteur sera débité du montant du paiement le jour de la commande (ou le lendemain en fonction de l'acquéreur).

Le débit de la première échéance de l'abonnement sera réalisé une fois la date d'effet atteinte, entre 00h00 et 05h00.

Si la date d'effet est positionnée au jour de la commande, l'acheteur sera débité 2 jours de suite (à J pour le paiement et à J+1 pour la première échéance).



Si vous souhaitez que le paiement réalisé le jour de la commande corresponde à la première échéance de l'abonnement, vous devez adapter la date d'effet. Par exemple, pour un abonnement mensuel, valorisez la date d'effet à J+30 lors de la demande de création d'abonnement.

A chaque échéance :

1. La plateforme de paiement réalise une demande d'autorisation pour le montant de l'échéance, en fournissant l'identifiant de transaction initiale (CIT) comme référence de chaînage.

Tous droits réservés

2. L'émetteur reconnaît la transaction comme une **MIT** faisant partie d'une série de paiements pour laquelle le porteur s'est authentifié préalablement et procède à la demande d'autorisation.

   La transaction ne sera pas refusée pour défaut d'authentification (soft decline).

3. Si le marchand a activé la règle de notification **URL de notification à la création d'un abonnement**, la plateforme de paiement notifie le site marchand du résultat du paiement.

L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias et de la transaction.

En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) la plateforme utilisera par défaut l'identifiant de transaction émetteur comme référence de chaînage si nécessaire.

Dans le cas où le marchand duplique (**MIT**) la transaction créée le jour de la commande, la plateforme utilise automatiquement cet identifiant comme référence de chaînage.

Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

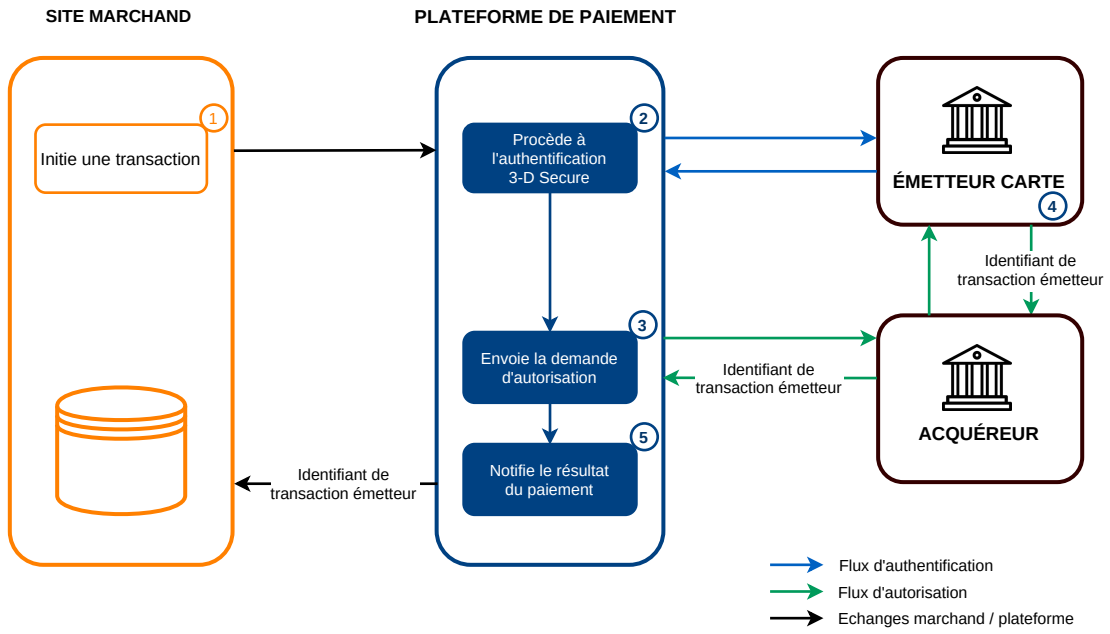
5.6. Paiement par alias

Le paiement par alias permet à partir d'un alias préalablement enregistré, la réalisation de paiements unitaires ou multiples sans avoir à sélectionner un moyen de paiement et de saisir des données bancaires.

Dans ce cas, une simple étape de confirmation est présentée avec un récapitulatif de la transaction (numéro et montant).

Schéma simplifié

CIT



1. Le site marchand soumet une demande de paiement avec réutilisation d'un alias.

   L'acheteur vérifie les informations affichées sur la page de paiement, saisit le CVV de sa carte puis valide.

   > Lorsque l'alias est associé à un moyen de paiement expiré, la plateforme propose automatiquement à l'acheteur de renseigner les nouvelles données bancaires afin de réaliser le paiement et mettre à jour l'alias qui lui est associé.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   > La réglementation impose la saisie du CVV et une authentification du porteur pour ce cas d'usage.
   >
   > L'authentification est réalisée sur le montant du paiement.

3. Une fois l'authentification (challenge ou frictionless) terminée, la plateforme procède à la demande d'autorisation en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande d'autorisation.
5. La plateforme de paiement notifie le site marchand du résultat.

   La plateforme affiche le ticket à l'acheteur.

   Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail la confirmation du paiement.

Tous droits réservés

L'identifiant de transaction émetteur est stocké par la plateforme de paiement.

Dans le cas où le marchand duplique (**MIT**) la transaction, la plateforme utilisera automatiquement cet identifiant comme référence de chaînage.

Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

Tous droits réservés

5.7. Utilisation d'un alias pour souscrire à un abonnement

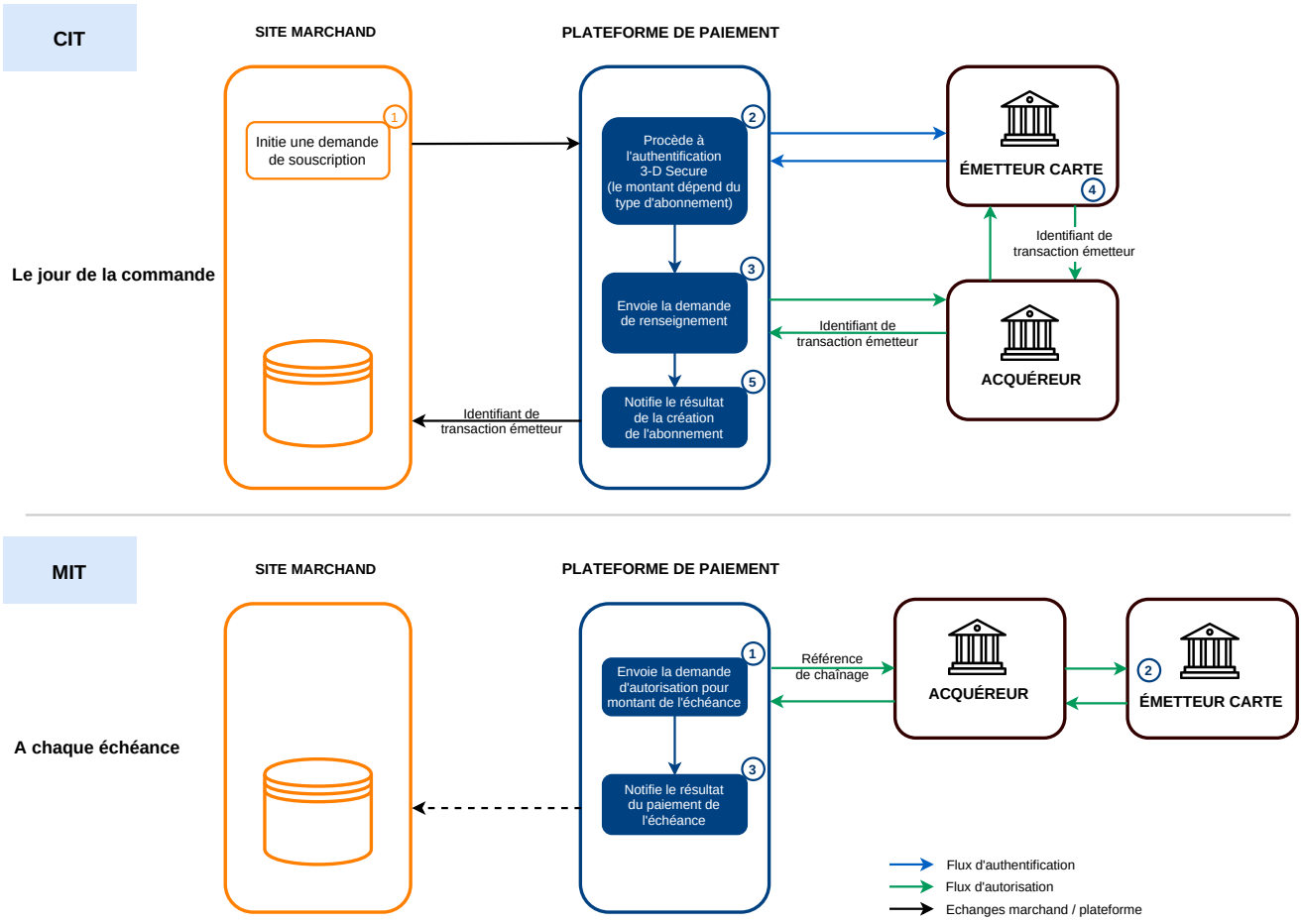
Une fois un alias créé, il est possible d'ajouter un ou plusieurs abonnement(s) supplémentaire(s) qui utiliseront cet alias.

À la souscription d'un nouvel abonnement, aucune saisie de données bancaires ne sera demandée. Seule une confirmation de la part de l'acheteur sera requise.

Aucun paiement ne sera réalisé lors de la souscription. Seule une demande de renseignement est réalisée afin de valider les données du moyen de paiement.

Le premier paiement sera réalisé une fois la date d'effet atteinte, entre 00h00 et 05h00.

Schéma simplifié



Le jour de la commande :

1. Le site marchand soumet une demande de souscription à un abonnement à partir d'un alias existant.

   L'acheteur vérifie les données de l'abonnement puis valide.

2. La plateforme de paiement notifie le site marchand du résultat.

   La plateforme affiche le ticket à l'acheteur. Il contient notamment les montants de l'abonnement.

   Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail la confirmation de l'enregistrement de l'abonnement.

A chaque échéance :

1. La plateforme de paiement réalise une demande d'autorisation pour le montant de l'échéance, en fournissant l'identifiant de transaction initiale (CIT) comme référence de chaînage.
2. L'émetteur reconnaît la transaction comme une **MIT** faisant partie d'une série de paiements pour laquelle le porteur s'est authentifié préalablement et procède à la demande d'autorisation.

   La transaction ne sera pas refusée pour défaut d'authentification (soft decline).
3. Si le marchand a activé la règle de notification **URL de notification à la création d'un abonnement**, la plateforme de paiement notifie le site marchand du résultat du paiement.

Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

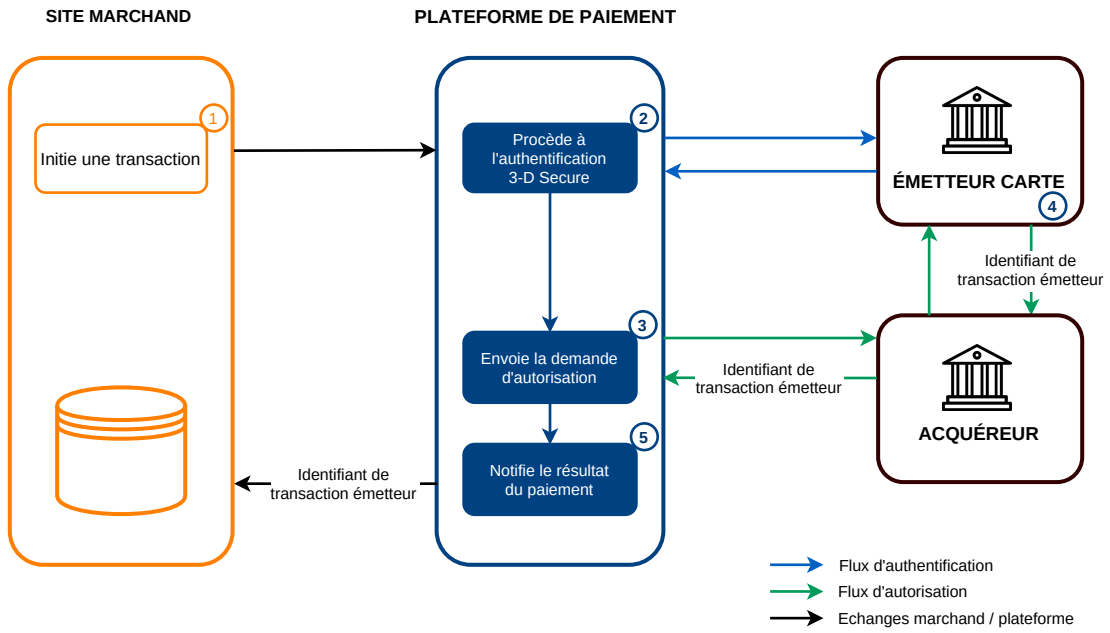
Tous droits réservés

5.8. Paiement avec proposition au porteur de créer un alias

L'acheteur a la possibilité, au moment du paiement, de mémoriser ses données bancaires en cochant la case correspondante. Cette opération, totalement sécurisée, permet à l'acheteur de faciliter ses futurs achats.

Schéma simplifié

CIT



1. Le site marchand soumet une demande de paiement.

   L'acheteur sélectionne le moyen de paiement à enregistrer et renseigne les données de son moyen de paiement.

   Par l'intermédiaire d'une case à cocher, l'acheteur peut donner son accord afin que son moyen de paiement soit enregistré par la plateforme de paiement. Par défaut, cette case n'est pas cochée.

2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   > Si l'acheteur a coché la case, un alias du moyen de paiement est créé. Une authentification forte est imposée par la réglementation.
   >
   > Dans le cas contraire, l'acheteur est soumis à une authentification avec ou sans interaction.
   >
   > Quel que soit le choix de l'acheteur, l'authentification est réalisée sur le montant du paiement.

3. Une fois l'authentification terminée, la plateforme procède à la demande d'autorisation en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans la réponse à la demande d'autorisation.
5. La plateforme de paiement notifie le site marchand du résultat.

   > L'alias (token) ne sera pas créé si la demande d'autorisation ou de renseignement est refusée.

   La plateforme affiche le ticket à l'acheteur. Il contient notamment :

   - le résultat du paiement,
   - l'alias éventuellement créé.

Tous droits réservés

Si vous avez configuré les règles de notification correspondantes, l'acheteur recevra par e-mail :

- le ticket de paiement
- la confirmation de l'enregistrement de ses informations bancaires sur la plateforme de paiement de la boutique,
- son alias (token) qu'il pourra utiliser ultérieurement pour effectuer une autre opération bancaire.

L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias et de la transaction.

En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) la plateforme utilisera par défaut l'identifiant de transaction émetteur comme référence de chaînage si nécessaire.

Dans le cas où le marchand duplique (**MIT**) la transaction créée le jour de la commande, la plateforme utilise automatiquement cet identifiant comme référence de chaînage.

Dans ce cas d'usage, la gestion de la référence de chaînage est transparente pour le marchand.

Tous droits réservés

6. CYCLE DE VIE D'UN PAIEMENT RÉCURRENT

L'abonnement démarre à sa date d'effet.

La plateforme de paiement va alors créer les paiements en suivant l'échéancier déterminé par la règle de l'abonnement envoyée dans le formulaire de création de l'abonnement (champ vads_sub_desc).

Dans le cadre de l'application de la DSP2, la plateforme de paiement transmet, dans la demande d'autorisation, une référence de chaînage, afin d'éviter les refus pour défaut d'authentification (soft decline).

A chaque échéance d'un abonnement, si la règle **URL de notification à la création d'un abonnement** est activée et correctement configurée, le site marchand recevra le résultat du paiement sur son URL de notification (IPN).

La notification contient notamment :

- le champ **vads_subscription**, qui indique la référence de l'abonnement,
- le champ **vads_recurrence number**, qui indique le numéro de l'échéance,
- le champ **vads_occurrence_type**, qui indique de quelle échéance il s'agit (première, énième ou dernière échéance),
- le champ **vads_trans_status** qui indique le statut du paiement (accepté ou refusé).

En cas de paiement refusé :

- le marchand ne sera pas averti par e-mail,
- le paiement ne sera pas représenté automatiquement.

Si le moyen de paiement a atteint sa date d'expiration, une transaction refusée est créée sans appel à la banque émettrice. Le détail de l'erreur (vads_payment_error) est valorisé à 8 - La date d'expiration de la carte ne permet pas cette action.

Si les données du moyen de paiement ont été purgées suite à une inactivité de 15 mois, une transaction refusée est créée sans appel à la banque émettrice. Le détail de l'erreur (vads_payment_error) est valorisé à 107 - Le moyen de paiement associé à l'alias n'est plus valide.

Cas particulier des récurrences à fréquence quotidienne

Si vous demandez la création d'un abonnement pour débiter le porteur tous les jours (RRULE:FREQ=DAILY;INTERVAL=1), et que la date d'effet demandée (vads_sub_effect_date) correspond à la date de création de l'abonnement, alors lorsque la plateforme de paiement va traiter cet abonnement le lendemain matin (entre minuit et 5h), 2 paiements seront créés :

- celui de la veille (correspondant à la date d'effet),
- et celui du jour.

Pour éviter cela, il est conseillé de transmettre une date d'effet au lendemain du jour de la création de l'abonnement.

6.1. Liste des codes retour de la demande d'autorisation

Les codes retour de la demande d'autorisation sont retournés par la banque émettrice (si disponible).

Valeur	Description	Rejeu autorisé
00	Transaction approuvée ou traitée avec succès	
02	Contacter l'émetteur de carte	
03	Accepteur invalide	OUI

Tous droits réservés

Valeur	Description	Rejeu autorisé
04	Conserver la carte	OUI
05	Ne pas honorer	OUI
07	Conserver la carte, conditions spéciales	OUI
08	Approuver après identification	
12	Transaction invalide	OUI
13	Montant invalide	OUI
14	Numéro de porteur invalide	OUI
15	Emetteur de carte inconnu	OUI
17	Annulation acheteur	
19	Répéter la transaction ultérieurement	
20	Réponse erronée (erreur dans le domaine serveur)	
24	Mise à jour de fichier non supportée	
25	Impossible de localiser l'enregistrement dans le fichier	
26	Enregistrement dupliqué, ancien enregistrement remplacé	
27	Erreur en « edit » sur champ de mise à jour fichier	
28	Accès interdit au fichier	
29	Mise à jour impossible	
30	Erreur de format	
31	Identifiant de l'organisme acquéreur inconnu	OUI
33	Date de validité de la carte dépassée	OUI
34	Suspicion de fraude	OUI
38	Date de validité de la carte dépassée	
41	Carte perdue	OUI
43	Carte volée	OUI
46	Compte client fermé	
51	Provision insuffisante ou crédit dépassé	
54	Date de validité de la carte dépassée	OUI
55	Code confidentiel erroné	
56	Carte absente du fichier	OUI
57	Transaction non permise à ce porteur	OUI
58	Transaction non permise à ce porteur	
59	Suspicion de fraude	OUI
60	L'accepteur de carte doit contacter l'acquéreur	
61	Montant de retrait hors limite	

Valeur	Description	Rejeu autorisé
63	Règles de sécurité non respectées	OUI
65	Nombre de retraits dépassé	
68	Réponse non parvenue ou reçue trop tard	
75	Nombre d'essais code confidentiel dépassé	
76	Porteur déjà en opposition, ancien enregistrement conservé	OUI
78	Transaction bloquée, première transaction sur carte non débloquée correctement	
80	Le paiement sans contact n'est pas admis par l'émetteur	
81	Le paiement non sécurisé n'est pas admis par l'émetteur	
82	CVV, dCVV, iCVV incorrect	
83	Révocation de tous les paiements par abonnement pour la carte	
84	R1 - Révocation paiement par abonnement pour la carte chez le marchand ou pour le MCC et la carte	
86	6P - Echec de la vérification des données par l'émetteur	
90	Arrêt momentané du système	
91	Émetteur de cartes inaccessible	
94	Transaction dupliquée	
96	Mauvais fonctionnement du système	
97	Échéance de la temporisation de surveillance globale	
98	Serveur indisponible routage réseau demandé à nouveau	
99	Incident domaine initiateur	

6.2. Notification par e-mail en cas de refus d'une échéance

Cas de l’option Autorisation anticipée

Lorsque le paiement est refusé, un e-mail d’avertissement est envoyé au marchand.

7. PROPOSER DES TENTATIVES DE PAIEMENT SUPPLÉMENTAIRES

Lorsqu'un paiement est refusé, vous avez la possibilité de proposer à l'acheteur de retenter avec un autre moyen de paiement.

Le nombre de tentatives supplémentaires est paramétrable depuis le Back Office Expert :

1. Ouvrez le menu **Paramétrage** > **Boutique** puis cliquez sur le nom de la boutique sur laquelle la configuration doit être modifiée.
2. Sélectionnez l'onglet **Configuration**.
3. Renseignez le nombre de tentatives supplémentaires autorisées en cas de refus de paiement.

   Si vous paramétrez 2 tentatives supplémentaires, alors l'acheteur pourra réaliser au total 3 tentatives de paiement.
4. Si vous le souhaitez, vous pouvez activer l'envoi d'une notification de fin de paiement (IPN) à chaque tentative refusée, en cochant la case **URL de notification sur tentative refusée**.
5. Cliquez sur le bouton **Sauvegarder**.

Les tentatives supplémentaires ne sont pas proposées :

- si le marchand a demandé un retour automatique à la boutique via le champ **vads_redirect_error_timeout**,
- si le paiement est un paiement en N fois.

Tentatives de paiement supplémentaires et paiement par alias (1 clic).

Si un paiement 1 clic est refusé, l'acheteur sera invité à choisir un nouveau moyen de paiement et à saisir les données de sa carte.

Si le paiement est accepté :

- la transaction ne sera pas associée à l'alias transmis dans la requête,
- l'alias ne sera pas mis à jour.

Tous droits réservés

8. ÉTABLIR LE DIALOGUE AVEC LA PLATEFORME DE PAIEMENT

Le dialogue entre le site marchand et la plateforme de paiement s'effectue par un échange de données.

Pour créer un paiement, ces données sont envoyées au moyen d'un formulaire HTML via le navigateur de l'acheteur.

A la fin du paiement, le résultat est transmis au site marchand de deux manières :

- Automatiquement grâce à des notifications appelées URL de notification instantanée (ou IPN pour Instant Payment Notification). Voir chapitre **Paramétrer les notifications**.
- Par le navigateur, lorsque l'acheteur clique sur le bouton pour revenir au site marchand. Voir chapitre **Gérer le dialogue vers le site marchand** .

Pour assurer la sécurité des échanges, les données sont signées au moyen d'une clé connue uniquement du marchand et de la plateforme de paiement.

8.1. Similarités avec le paiement unitaire

Toutes les fonctionnalités disponibles pour le paiement unitaire le sont également pour les paiements par alias et par abonnements.

Pour plus d'informations, référez-vous au *Guide d'implémentation API Formulaire*

En voici cependant une liste non-exhaustive :

- Paiement unitaire, réalisable en une fois, ou fractionné.
- Gestion de plusieurs devises.
- Gestion de plusieurs moyens de paiement et des contrats commerçants associés.
- Personnalisation des pages de paiements.

Tous droits réservés

9. CONFIGURER LES NOTIFICATIONS

Plusieurs types de notifications sont à disposition dans le Back Office Expert :

- Appel URL de notification
- E-mail envoyé au marchand
- E-mail envoyé à l'acheteur
- SMS envoyé au marchand
- SMS envoyé à l'acheteur

La notification est envoyée en fonction de l'événement qui a lieu (paiement accepté, abandon par l'acheteur, annulation par le marchand, etc.).

Les notifications de type Appel URL de notification sont les plus importantes. Elles sont l'unique moyen fiable pour le site marchand d'obtenir le résultat d'un paiement.

Échec URL de notification

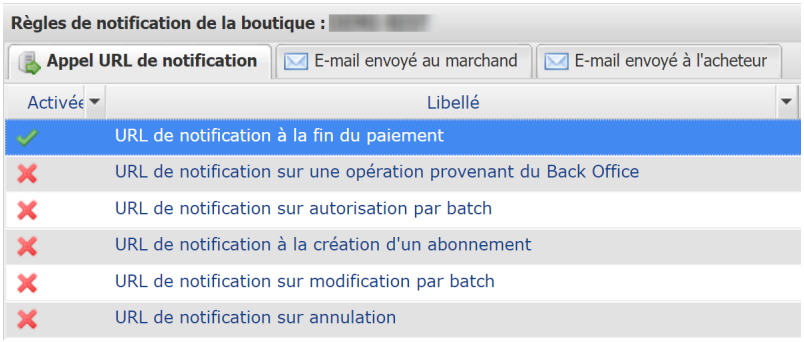
Si la plateforme n'arrive pas à joindre votre URL, elle envoie un e-mail à l'adresse spécifiée.

Cet e-mail contient :

- le code HTTP de l'erreur rencontrée ;
- des éléments d'analyse en fonction de l'erreur ;
- les conséquences de l'erreur ;
- la procédure à suivre depuis le Back Office Expert pour renvoyer la requête vers l'URL déjà définie.

Accés à la gestion des règles de notification

1. Connectez-vous à votre Back Office Marchand :
   https://secure.lyra.com/portal/
2. Cliquez sur le bouton **Autres actions** pour accéder au Back Office Expert.
3. Allez dans le menu **Paramétrage** > **Règles de notifications**.



Tous droits réservés

9.1. Configurer la notification à la fin du paiement

La plateforme de paiement notifie le site marchand dans les cas suivants :

- Paiement accepté
- Paiement refusé
- Création ou mise à jour d'un alias
- Création d'un abonnement

Cette notification est indispensable pour communiquer le résultat d'une demande de paiement, de création d'alias ou de création d'abonnement.

Elle informera le site marchand du résultat même si l'acheteur ne clique pas sur le bouton Retour à la boutique.

1. Effectuez un clic droit sur la ligne **URL de notification à la fin du paiement**.
2. Sélectionnez **Gérer la règle**.
3. Renseignez le champ **Adresse(s) e-mail(s) à avertir en cas d'échec** dans l'encadré **Paramétrage général**. Séparez les adresses e-mails par un point virgule (;).
4. Cochez la case **Rejeu automatique en cas d'échec** si vous souhaitez autoriser la plateforme à renvoyer automatiquement la notification en cas d'échec, et ce, jusqu'à 4 fois.

   Pour plus d'informations, reportez-vous au chapitre Rejeu automatique en cas d'échec à la page 44.
5. Pour recevoir les notifications au format API Formulaire, renseignez l'URL de votre page dans les champs **URL à appeler en mode TEST** et **URL à appeler en mode PRODUCTION** dans la section "URL de notification de l'API formulaire V1, V2".
6. Sauvegardez vos modifications.

9.2. Configurer la notification en cas d'abandon ou annulation

La plateforme de paiement notifie le site marchand dans les cas suivants :

- En cas d'abandon ou annulation de la part de l'acheteur, via le bouton **Annuler et retourner à la boutique**.
- Lorsque l'acheteur n'a pas terminé son paiement avant l'expiration de sa session de paiement.

  La durée maximale d'une session de paiement est de 10 minutes.

Ce paramétrage est obligatoire si vous utilisez le moyen de paiement **FacilyPay Oney**.

Cette règle est désactivée par défaut.

1. Effectuez un clic droit sur la ligne **URL de notification sur annulation**.
2. Sélectionnez **Gérer la règle**.
3. Renseignez le champ **Adresse(s) e-mail(s) à avertir en cas d'échec** dans l'encadré **Paramétrage général**. Séparez les adresses e-mails par un point virgule (;).
4. Cochez **Rejeu automatique en cas d'échec** pour activer jusqu'à 4 tentatives de renvoi automatique par la plateforme.

   Pour plus d'informations, voir Rejeu automatique en cas d'échec à la page 44.
5. Pour recevoir les notifications au format API Formulaire, renseignez l'URL de votre page dans les champs **URL à appeler en mode TEST** et **URL à appeler en mode PRODUCTION** dans la section "URL de notification de l'API formulaire V1, V2".
6. Pour le client JavaScript, renseignez l'URL de votre page dans les champs **URL cible de l'IPN à appeler en mode TEST** et **URL cible de l'IPN à appeler en mode PRODUCTION** dans la section "URL de notification de l'API REST".
7. Sauvegardez vos modifications.
8. Activez la règle, faites un clic droit sur **URL de notification sur annulation** et sélectionnez **Activer la règle**.

9.3. Configurer la notification sur une opération provenant du Back Office

Cette règle permet de notifier le site marchand à chaque opération réalisée depuis le Back Office Expert :

- Création d'un paiement manuel (accepté ou refusé)
- Modification d'une transaction
- Duplication d'une transaction
- Remboursement d'une transaction
- Annulation d'une transaction
- Validation d'une transaction
- Création d'un alias
- Mise à jour d'un alias

1. Effectuez un clic droit sur la ligne **URL de notification sur une opération provenant du Back Office**.
2. Sélectionnez **Gérer la règle**.
3. Renseignez le champ **Adresse(s) e-mail(s) à avertir en cas d'échec** dans l'encadré **Paramétrage général**. Séparez les adresses e-mails par un point virgule (;).
4. Cochez **Rejeu automatique en cas d'échec** pour activer jusqu'à 4 tentatives de renvoi automatique par la plateforme.
   Pour plus d'informations, voir Rejeu automatique en cas d'échec à la page 44.
5. Pour recevoir les notifications au format API Formulaire, renseignez l'URL de votre page dans les champs **URL à appeler en mode TEST** et **URL à appeler en mode PRODUCTION** dans la section "URL de notification de l'API formulaire V1, V2".
6. Pour le client JavaScript, renseignez l'URL de votre page dans les champs **URL cible de l'IPN à appeler en mode TEST** et **URL cible de l'IPN à appeler en mode PRODUCTION** dans la section "URL de notification de l'API REST".
7. Sauvegardez vos modifications.
8. Activez la règle, en effectuant un clic droit sur **URL de notification sur une opération provenant du Back Office** et en sélectionnant **Activer la règle**.

Tous droits réservés

9.4. Configurer la notification à la création d'un abonnement

La plateforme de paiement notifie le site marchand dans les cas suivants :

- Lorsque la plateforme de paiement crée une nouvelle échéance d'un paiement récurrent.
- A chaque nouvelle tentative de paiement, après qu'une échéance d'un paiement récurrent a été refusée.

  Nécessite l'activation de l'option autorisation anticipée.

Cette règle est désactivée par défaut.

1. Effectuez un clic droit sur la ligne **URL de notification à la création d'un abonnement**.
2. Sélectionnez **Gérer la règle**.
3. Renseignez le champ **Adresse(s) e-mail(s) à avertir en cas d'échec** dans l'encadré **Paramétrage général**. Séparez les adresses e-mails par un point virgule (;).
4. Cochez la case **Rejeu automatique en cas d'échec** si vous souhaitez autoriser la plateforme à renvoyer automatiquement la notification en cas d'echec, et ce, jusqu'à 4 fois.

   Pour plus d'informations, reportez-vous au chapitre Rejeu automatique en cas d'échec à la page 44.
5. Pour recevoir les notifications au format API Formulaire, renseignez l'URL de votre page dans les champs **URL à appeler en mode TEST** et **URL à appeler en mode PRODUCTION** dans la section "URL de notification de l'API formulaire V1, V2".
6. Pour le client JavaScript, renseignez l'URL de votre page dans les champs **URL cible de l'IPN à appeler en mode TEST** et **URL cible de l'IPN à appeler en mode PRODUCTION** dans la section "URL de notification de l'API REST".
7. Sauvegardez vos modifications.
8. Activez la règle, en effectuant un clic droit sur **URL de notification à la création d'un abonnement** et en sélectionnant **Activer la règle**.

9.5. Configurer la notification sur autorisation par batch

Si la boutique dispose de l'option **Autorisation anticipée**, il est nécessaire d'activer la règle **URL de notification sur autorisation par batch** afin de recevoir le résultat final du paiement.

Cette règle est désactivée par défaut.

1. Effectuez un clic droit sur la ligne **URL de notification sur autorisation par batch**.
2. Sélectionnez **Gérer la règle**.
3. Renseignez le champ **Adresse(s) e-mail(s) à avertir en cas d'échec** dans l'encadré **Paramétrage général**. Séparez les adresses e-mails par un point virgule (;).
4. Cochez la case **Rejeu automatique en cas d'échec** si vous souhaitez autoriser la plateforme à renvoyer automatiquement la notification en cas d'echec, et ce, jusqu'à 4 fois.
   Pour plus d'informations, reportez-vous au chapitre Rejeu automatique en cas d'échec à la page 44.
5. Pour recevoir les notifications au format API Formulaire, renseignez l'URL de votre page dans les champs **URL à appeler en mode TEST** et **URL à appeler en mode PRODUCTION** dans la section "URL de notification de l'API formulaire V1, V2".
6. Pour le client JavaScript, renseignez l'URL de votre page dans les champs **URL cible de l'IPN à appeler en mode TEST** et **URL cible de l'IPN à appeler en mode PRODUCTION** dans la section "URL de notification de l'API REST".
7. Sauvegardez vos modifications.
8. Activez la règle, en effectuant un clic droit sur **URL de notification sur autorisation par batch** et en sélectionnant **Activer la règle**.

9.6. Rejeu automatique en cas d'échec

Les notifications déclenchées manuellement depuis le Back Office Expert ne sont pas concernées par le rejeu automatique.

Vous pouvez activer une option permettant à la plateforme de paiement de renvoyer automatiquement les notifications lorsque votre site est temporairement injoignable. Cette option effectue jusqu'à quatre tentatives de renvoi.

Une notification est considérée comme échouée si le code retour HTTP renvoyé par votre site ne correspond pas à l'un des codes suivants : **200**, **201**, **202**, **203**, **204**, **205**, **206**, **301**, **302**, **303**, **307**, **308**.

Les tentatives d'appel s'effectuent à des heures fixes toutes les 15 minutes (00, 15, 30, 45).

Après chaque tentative infructueuse, la plateforme envoie un e-mail d'alerte à l'adresse configurée dans la règle de notification.

L'objet de l'e-mail d'alerte contient le numéro de la tentative, présenté sous la forme attempt # suivi du numéro de tentative.

- Exemple d'objet d'un e-mail d'alerte reçu suite au premier échec de notification à la fin d'un paiement :

```
[MODE TEST] Ma Boutique - Tr. réf. 067925 / ECHEC lors de l'appel de votre URL de
 notification [unsuccessful attempt #1]
```

- Exemple d'objet d'e-mail reçu lors d'un deuxième échec :

```
[MODE TEST] Ma Boutique - Tr. réf. 067925 / ECHEC lors de l'appel de votre URL de
 notification [unsuccessful attempt #2]
```

- Exemple d'objet d'e-mail reçu lors d'un troisième échec :

```
[MODE TEST] Ma Boutique - Tr. réf. 067925 / ECHEC lors de l'appel de votre URL de
 notification [unsuccessful attempt #3]
```

- Exemple d'objet d'e-mail reçu lors de la dernière tentative :

```
[MODE TEST] Ma Boutique - Tr. réf. 067925 / ECHEC lors de l'appel de votre URL de
 notification [unsuccessful attempt #last]
```

  Pour notifier au site marchand l'échec de la dernière tentative de notification, l'objet de l'e-mail comportera la mention attempt #last.

Lors du rejeu automatique, certaines informations ne sont pas enregistrées en base de données ou sont modifiées.

Exemples de champs non disponibles ou non enregistrés en base de données :

Nom du champ	Description
vads_page_action	Opération réalisée
vads_payment_config	Typologie de paiement (comptant ou en plusieurs échéances)
vads_action_mode	Mode d'acquisition des informations du moyen de paiement

Exemples de champs envoyés avec des valeurs différentes :

Nom du champ	Nouvelle valeur
vads_url_check_src	Toujours valorisé à RETRY lors d'un rejeu automatique.
vads_trans_status	Le statut de la transaction peut varier entre l'appel initial et le rejeu automatique (annulation du marchand, remise en banque de la transaction, etc.).

Nom du champ	Nouvelle valeur
vads_hash	La valeur de ce champ est regénérée à chaque appel.
signature	La valeur de la signature dépend des différents statuts qui peuvent varier entre l'appel initial et le rejeu automatique.

Ces e-mails détaillent :

- Le problème rencontré,
- Des éléments d'analyse en fonction de l'erreur,
- Ses conséquences,
- La procédure à suivre depuis le Back Office Expert pour déclencher manuellement la notification.

Après la quatrième tentative, il est toujours possible de rejouer l'URL de notification manuellement depuis votre Back Office Expert.

Attention, pendant la période de rejeu automatique, tout appel manuel à l'URL de notification influera sur le nombre de tentatives automatiques :

- Un appel manuel réussi provoque l'arrêt du rejeu automatique ;
- Un appel manuel en échec n'a aucun impact sur le rejeu automatique en cours.

Tous droits réservés

9.7. Configurer les e-mails envoyés à l'acheteur

1. Connectez-vous à votre Back Office Expert :
   https://secure.lyra.com/portal/

2. Cliquez sur **Autres actions** en bas du menu pour accéder à votre Back Office Expert.

   > **Autres actions** apparaît uniquement si votre compte utilisateur dispose de la permission "Accès au back office expert".
   >
   > Rapprochez-vous du Gestionnaire du back office de votre société pour obtenir cette permission.

3. Ouvrez le menu **Paramétrage** > **Règles de notifications**, onglet **E-mail envoyé à l'acheteur**.

4. Effectuez un clic droit sur la règle à modifier et sélectionnez **Activer la règle**.

5. Effectuez un nouveau clic droit sur la règle et sélectionnez **Gérer la règle**.
   L'assistant de gestion d'une règle de notification s'affiche.

6. Dans l'encadré **Paramétrage général**, personnalisez le libellé de la règle si besoin.

7. Pour personnaliser le contenu de l'e-mail:
   a. Cliquez sur **Paramétrage e-mail acheteur**.
   b. Sélectionnez le modèle d'e-mail à appliquer
   c. Sélectionnez la langue à modifier
   d. Cliquez sur le lien **Personnaliser des valeurs de texte par défaut** pour modifier l'objet et le contenu de l'e-mail par défaut.
   e. Cliquez sur **Champs à inclure** pour afficher la liste des champs disponibles pour personnaliser l'e-mail.
   f. Sélectionnez les champs à inclure. Un récapitulatif détaillé du traitement de la demande sera ajouté au contenu de l'e-mail.

   > Pour visualiser au préalable les modifications effectuées, cliquez sur **Prévisualiser l'e-mail** situé en bas de la boîte de dialogue.

8. Modifiez les condictions de notifications :
   a. Cliquez sur **Conditions de la règle**
      Une condition est constituée d'une variable, d'un opérateur de comparaison et d'une valeur de référence.
      Exemple : "mode = TEST", "montant supérieur à 1000". Lors de l'exécution d'une règle, la valeur de la variable est récupérée et comparée à la valeur de référence.
   b. Double-cliquez sur une condition existante pour la modifier.
   c. Cliquez sur **Ajouter** pour créer une nouvelle condition.
      Toutes les conditions doivent être validées pour que la règle soit exécutée.

9. Cliquez sur **Sauvegarder**.

Tous droits réservés

10. GÉNÉRER UN FORMULAIRE DE PAIEMENT

Vous devez construire un formulaire HTML comme suit :

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
 <input type="hidden" name="parametre1" value="valeur1" />
 <input type="hidden" name="parametre2" value="valeur2" />
 <input type="hidden" name="parametre3" value="valeur3" />
 <input type="hidden" name="signature" value="signature"/>
 <input type="submit" name="payer" value="Payer"/>
</form>
```

Les éléments techniques :

- Les balises `<form>` et `</form>` servent à créer un formulaire HTML.
- L'attribut `method="POST"` définit la méthode utilisée pour envoyer les données.
- L'attribut `action="https://secure.lyra.com/vads-payment/"` indique la destination des données du formulaire.

Les données du formulaire :

- L'identifiant de la boutique.
- Les caractéristiques du paiement selon le cas d'utilisation.
- Les informations complémentaires adaptées à vos besoins.
- La signature garantissant l'intégrité du formulaire.

Utilisez la balise `<input>` pour ajouter des données au formulaire :

`<input type="hidden" name="parametre1" value="valeur1"/>`

Consultez le Dictionnaire de données pour définir les attributs `name` et `value`.

Encodez toutes les données du formulaire en UTF-8.

Cela garantit que les caractères spéciaux (accents, ponctuation, etc.) sont correctement interprétés par la plateforme de paiement. Un encodage incorrect entraîne un calcul de signature erroné et le rejet du formulaire.

Le bouton **Payer** pour envoyer des données :

`<input type="submit" name="payer" value="Payer"/>`

Les cas d'utilisation présentés dans les chapitres suivants vous permettront de construire votre formulaire de paiement en fonction de vos besoins.

Indications sur les différents formats possibles lors de la construction de votre formulaire :

Notation	Description
a	Caractères alphabétiques (de 'A' à 'Z' et de 'a' à 'z')
n	Caractères numériques
s	Caractères spéciaux
an	Caractères alphanumériques
ans	Caractères alphanumériques et spéciaux (à l'exception de `<` et `>`)
3	Longueur fixe de 3 caractères
..12	Longueur variable jusqu'à 12 caractères
json	JavaScript Object Notation. Objet contenant des paires de clé/valeur séparées par une virgule `,`. Il commence par une accolade gauche `{` et se termine par une accolade droite `}`.

Notation	Description
	Format des paires clé-valeur : • Chaque paire clé-valeur suit la syntaxe : `"nom_de_clé": valeur`. • Le nom de la clé doit être alphanumérique. Types de valeurs possibles : • Chaîne de caractères (encadrée par des guillemets anglais). • Nombre. • Objet. • Tableau. • Booléen. • Valeur vide. Exemple : `{"name1":45,"name2":"value2", "name3":false}`
bool	Booléen. Peut prendre la valeur `true` ou `false`.
enum	Caractérise un champ possédant un nombre fini de valeurs. La liste des valeurs possibles est donnée dans la définition du champ.
liste d'enum	Liste de valeurs séparées par un " `;` ". La liste des valeurs possibles est donnée dans la définition du champ. Exemple : `vads_available_languages=fr;en`
map	Liste de paires clé-valeur séparées par un " `;` ". Chaque paire clé-valeur contient le nom de la clé suivi par " `=` " et une valeur. La valeur peut être : • Une chaîne de caractères. • Un booléen. • Un objet json. • Un objet xml. La liste des valeurs possibles pour chaque paire de clé-valeur est donnée dans la définition du champ. Exemple : `vads_theme_config=SIMPLIFIED_DISPLAY=true;RESPONSIVE_MODEL=Model_1`

10.1. Créer un formulaire 'Création de l'alias sans paiement'

Cas d'utilisation : création d'un alias pour effectuer des paiements rapides ultérieurement.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser	enum	REGISTER
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_currency	Code numérique de la monnaie à utiliser pour le paiement, selon la norme ISO 4217 (code numérique).	n3	Ex : 978 pour l'euro (EUR)
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

2. Utilisez le champ **vads_identifier** si vous souhaitez générer l'identifiant du token associé au moyen de paiement.
   Le format du token ne doit pas être an..32. Ce format est réservé aux tokens générés par la plateforme de paiement.

3. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Création d'un alias sans paiement à la page 78.

10.2. Créer un formulaire 'Modification des informations associées à l'alias'

Cas d'utilisation : mise à jour des informations bancaires associées à un alias.

Tous droits réservés

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser.	enum	**REGISTER_UPDATE**
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_identifier	Alias (unique) associé à un moyen de paiement.	ans..50	Ex : MonAlias **Remarque** : deux formats possibles : • **an32** : lorsque l'alias est généré par la plateforme • **ans..50** : lorsque l'alias est généré par le marchand
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

2. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Modification des informations associées à l'alias à la page 83.

Tous droits réservés

10.3. Créer un formulaire 'Création de l'alias lors d'un paiement'

Cas d'utilisation : paiement avec création d'un alias.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser	enum	REGISTER_PAY
vads_amount	Montant du paiement dans sa plus petite fraction monétaire (le centime pour l'euro) .	n..12	Ex : 4525 pour 45,25 EUR
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_currency	Code numérique de la monnaie à utiliser pour le paiement, selon la norme ISO 4217 (code numérique).	n3	Ex : 978 pour l'euro (EUR)
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_payment_config	Type de paiement	enum	SINGLE
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_trans_id	Numéro de la transaction. Doit être unique sur une même journée (de 00:00:00 UTC à 23:59:59 UTC).	an6	Ex : xrT15p
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

2. Utilisez le champ **vads_identifier** si vous souhaitez générer l'identifiant du token associé au moyen de paiement.

   Le format du token ne doit pas être an..32. Ce format est réservé aux tokens générés par la plateforme de paiement.

Tous droits réservés

3. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Création de l'alias lors d'un paiement à la page 87.

Tous droits réservés

10.4. Créer un formulaire 'Création de l'alias lors de la souscription à un abonnement'

Cas d'utilisation : souscription à un abonnement avec création d'un alias.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

Aucun paiement ne sera réalisé lors de la souscription. Seule une demande de vérification sera réalisée afin de valider les données du moyen de paiement.

Le premier paiement sera réalisé une fois la date d'effet atteinte, entre 00h00 et 05h00.

Si vous souhaitez que l'acheteur règle une première échéance au moment de la souscription, reportez vous au chapitre suivant : **Créer un formulaire 'Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement' à la page 55**.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser	enum	REGISTER_SUBSCRIBE
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_sub_amount	Montant des échéances de l'abonnement (dans sa plus petite fraction monétaire). **Le montant des échéances ne peut être valorisé à 0.**	n..12	Ex : 4525 pour 45,25 EUR
vads_sub_effect_date	Date de début de l'abonnement (ou date d'effet) dans le fuseau UTC, au format AAAAMMJJ.	n8	Ex : 20210601
vads_sub_currency	Code de la devise utilisée pour l'abonnement.	n3	Ex : 978 pour l'euro (EUR)
vads_sub_desc	Règle de récurrence à appliquer suivant la spécification iCalendar RFC5545. Si vous demandez la création d'un abonnement pour débiter le porteur tous les jours (RRULE:FREQ=DAILY;INTERV	string	La fréquence de l'abonnement peut être journalière, hebdomadaire ou mensuelle. Il est possible de spécifier le numéro du jour ou du mois (par exemple "le 10 du mois", "tous les 3 mois"). *Remarque: la chaîne ne doit pas contenir d'espace.* Exemples:

Nom du champ	Description	Format	Valeur

	et que la date d'effet demandée (vads_sub_effect_date) correspond à la date de création de l'abonnement, alors lorsque la plateforme de paiement va traiter cet abonnement le lendemain matin (entre 00:00 et 05:00), deux paiements seront créés :
	• celui de la veille (correspondant à la date d'effet)
	• celui du jour
	Pour éviter cela, il est recommandé de transmettre une date d'effet au lendemain du jour de la création de l'abonnement.
			• Pour définir un abonnement toutes les semaines :
			`RRULE:FREQ=WEEKLY`
			• Pour définir un abonnement toutes les deux semaines, aujourd'hui et tous les 7 jours :
			`RRULE:FREQ=WEEKLY;INTERVAL=2`
			• Pour définir des échéances de paiement ayant lieu le dernier jour de chaque mois, pendant 12 mois :
			`RRULE:FREQ=MONTHLY;`
			`BYMONTHDAY=28,29,30,31;`
			`BYSETPOS=-1;COUNT=12`
			• Pour définir des échéances de paiement ayant lieu le 10 de chaque mois, pendant 12 mois :
			`RRULE:FREQ=MONTHLY;`
			`COUNT=12;BYMONTHDAY=10`

vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

La valeur de **vads_sub_effect_date** ne doit pas être dans le passé.

2. Utilisez le champ **vads_identifier** si vous souhaitez générer l'identifiant du token associé au moyen de paiement.

   Le format du token ne doit pas être an..32. Ce format est réservé aux tokens générés par la plateforme de paiement.

3. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Création de l'alias lors de la souscription à un abonnement à la page 92.

10.5. Créer un formulaire 'Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement'

Cas d'utilisation : paiement et une souscription à un abonnement avec création d'un alias.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser	enum	REGISTER_PAY_SUBSCRIBE
vads_amount	Montant du paiement dans sa plus petite fraction monétaire (le centime pour l'euro) .	n..12	Ex : 4525 pour 45,25 EUR
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_currency	Code numérique de la monnaie à utiliser pour le paiement, selon la norme ISO 4217 (code numérique).	n3	Ex : 978 pour l'euro (EUR)
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_payment_config	Type de paiement	enum	SINGLE
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_sub_amount	Montant des échéances de l'abonnement (dans sa plus petite fraction monétaire). **Le montant des échéances ne peut être valorisé à 0.**	n..12	Ex : 4525 pour 45,25 EUR
vads_sub_currency	Code de la devise utilisée pour l'abonnement.	n3	Ex : 978 pour l'euro (EUR)
vads_sub_desc	Règle de récurrence à appliquer suivant la spécification iCalendar RFC5545. Si vous demandez la création d'un abonnement pour débiter le porteur tous les jours (RRULE:FREQ=DAILY;INTERV	string	La fréquence de l'abonnement peut être journalière, hebdomadaire ou mensuelle. Il est possible de spécifier le numéro du jour ou du mois (par exemple "le 10 du mois", "tous les 3 mois"). *Remarque: la chaîne ne doit pas contenir d'espace.* Exemples:

Nom du champ	Description	Format	Valeur

	et que la date d'effet demandée (vads_sub_effect_date) correspond à la date de création de l'abonnement, alors lorsque la plateforme de paiement va traiter cet abonnement le lendemain matin (entre 00:00 et 05:00), deux paiements seront créés :
	• celui de la veille (correspondant à la date d'effet)
	• celui du jour
	Pour éviter cela, il est recommandé de transmettre une date d'effet au lendemain du jour de la création de l'abonnement.
			• Pour définir un abonnement toutes les semaines :
			`RRULE:FREQ=WEEKLY`
			• Pour définir un abonnement toutes les deux semaines, aujourd'hui et tous les 7 jours :
			`RRULE:FREQ=WEEKLY;INTERVAL=2`
			• Pour définir des échéances de paiement ayant lieu le dernier jour de chaque mois, pendant 12 mois :
			`RRULE:FREQ=MONTHLY;`
			`BYMONTHDAY=28,29,30,31;`
			`BYSETPOS=-1;COUNT=12`
			• Pour définir des échéances de paiement ayant lieu le 10 de chaque mois, pendant 12 mois :
			`RRULE:FREQ=MONTHLY;`
			`COUNT=12;BYMONTHDAY=10`

vads_sub_effect_date	Date de début de l'abonnement (ou date d'effet) dans le fuseau UTC, au format AAAAMMJJ.	n8	Ex : 20210601
vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_trans_id	Numéro de la transaction. Doit être unique sur une même journée (de 00:00:00 UTC à 23:59:59 UTC).	an6	Ex : xrT15p
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

La valeur de **vads_sub_effect_date** ne doit pas être dans le passé.

2. Utilisez le champ **vads_identifier** si vous souhaitez générer l'identifiant du token associé au moyen de paiement.

Le format du token ne doit pas être an..32. Ce format est réservé aux tokens générés par la plateforme de paiement.

3. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement à la page 97.

10.6. Créer un formulaire 'Paiement par alias'

Cas d'utilisation : paiement en un clic (utilisation d'un alias existant et valide).

Dans le cadre de l'application de la DSP2, la saisie du CVV ainsi qu'une authentification du porteur sont requises lors d'un paiement par alias, dès lors que l'acheteur est présent. Le champ vads_threeds_mpi est pris en compte pour permettre une éventuelle authentification sans interaction.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser	enum	PAYMENT
vads_amount	Montant du paiement dans sa plus petite fraction monétaire (le centime pour l'euro) .	n..12	Ex : 4525 pour 45,25 EUR
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_currency	Code numérique de la monnaie à utiliser pour le paiement, selon la norme ISO 4217 (code numérique).	n3	Ex : 978 pour l'euro (EUR)
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_identifier	Alias (unique) associé à un moyen de paiement.	ans..50	Ex : MonAlias **Remarque** : deux formats possibles : • **an32** : lorsque l'alias est généré par la plateforme • **ans..50** : lorsque l'alias est généré par le marchand
vads_payment_config	Type de paiement	enum	SINGLE
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_trans_id	Numéro de la transaction. Doit être unique sur une même journée (de 00:00:00 UTC à 23:59:59 UTC).	an6	Ex : xrT15p
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

Tous droits réservés

2. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Paiement par alias à la page 102.

Tous droits réservés

10.7. Créer un formulaire 'Utilisation d'un alias pour souscrire à un abonnement'

Cas d'utilisation : utilisation d'un alias existant et valide pour souscrire à un abonnement.

Aucun paiement ne sera réalisé lors de la souscription.

Le premier paiement sera réalisé une fois la date d'effet atteinte, entre 00h00 et 05h00.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser.	enum	SUBSCRIBE
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_identifier	Alias (unique) associé à un moyen de paiement.	ans..50	Ex : MonAlias **Remarque** : deux formats possibles : • **an32** : lorsque l'alias est généré par la plateforme • **ans..50** : lorsque l'alias est généré par le marchand
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_sub_amount	Montant des échéances de l'abonnement (dans sa plus petite fraction monétaire). **Le montant des échéances ne peut être valorisé à 0.**	n..12	Ex : 4525 pour 45,25 EUR
vads_sub_effect_date	Date de début de l'abonnement (ou date d'effet) dans le fuseau UTC, au format AAAAMMJJ.	n8	Ex : 20210601
vads_sub_currency	Code de la devise utilisée pour l'abonnement.	n3	Ex : 978 pour l'euro (EUR)
vads_sub_desc	Règle de récurrence à appliquer suivant la spécification iCalendar RFC5545. Si vous demandez la création d'un abonnement pour débiter le porteur tous les jours (RRULE:FREQ=DAILY;INTERV et que la date d'effet demandée (vads_sub_effect_date)	string	La fréquence de l'abonnement peut être journalière, hebdomadaire ou mensuelle. Il est possible de spécifier le numéro du jour ou du mois (par exemple "le 10 du mois", "tous les 3 mois"). *Remarque: la chaîne ne doit pas contenir d'espace.* Exemples:

Nom du champ	Description	Format	Valeur

	correspond à la date de création de l'abonnement, alors lorsque la plateforme de paiement va traiter cet abonnement le lendemain matin (entre 00:00 et 05:00), deux paiements seront créés :
	• celui de la veille (correspondant à la date d'effet)
	• celui du jour
	Pour éviter cela, il est recommandé de transmettre une date d'effet au lendemain du jour de la création de l'abonnement.
			• Pour définir un abonnement toutes les semaines :
			`RRULE:FREQ=WEEKLY`
			• Pour définir un abonnement toutes les deux semaines, aujourd'hui et tous les 7 jours :
			`RRULE:FREQ=WEEKLY;INTERVAL=2`
			• Pour définir des échéances de paiement ayant lieu le dernier jour de chaque mois, pendant 12 mois :
			`RRULE:FREQ=MONTHLY;`
			`BYMONTHDAY=28,29,30,31;`
			`BYSETPOS=-1;COUNT=12`
			• Pour définir des échéances de paiement ayant lieu le 10 de chaque mois, pendant 12 mois :
			`RRULE:FREQ=MONTHLY;`
			`COUNT=12;BYMONTHDAY=10`

vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

La valeur de **vads_sub_effect_date** ne doit pas être dans le passé.

2. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

La liste des champs retournés dans la notification sont décrits dans le chapitre Souscription à un abonnement à la page 106.

10.8. Créer un formulaire 'Paiement avec proposition au porteur de créer un alias'

Cas d'utilisation : proposer la création d'un alias lors d'un paiement.

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors de l'enregistrement d'une carte. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

1. Utilisez l'ensemble des champs présents dans le tableau ci-après pour construire votre formulaire.

Nom du champ	Description	Format	Valeur
vads_page_action	Action à réaliser	enum	ASK_REGISTER_PAY
vads_amount	Montant du paiement dans sa plus petite fraction monétaire (le centime pour l'euro) .	n..12	Ex : 4525 pour 45,25 EUR
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
vads_currency	Code numérique de la monnaie à utiliser pour le paiement, selon la norme ISO 4217 (code numérique).	n3	Ex : 978 pour l'euro (EUR)
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_action_mode	Mode d'acquisition des données du moyen de paiement	enum	INTERACTIVE
vads_payment_config	Type de paiement	enum	SINGLE
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
vads_trans_id	Numéro de la transaction. Doit être unique sur une même journée (de 00:00:00 UTC à 23:59:59 UTC).	an6	Ex : xrT15p
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
signature	Signature garantissant l'intégrité des requêtes échangées entre le site marchand et la plateforme de paiement.	ans..44	Calculez la valeur du champ signature en utilisant l'ensemble des champs de votre formulaire, dont le nom commence par **vads_** (voir chapitre **Calculer la signature**).

2. Utilisez le champ **vads_identifier** si vous souhaitez générer l'identifiant du token associé au moyen de paiement.

   Le format du token ne doit pas être an..32. Ce format est réservé aux tokens générés par la plateforme de paiement.

3. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

Tous droits réservés

La liste des champs retournés dans la notification sont décrits dans le chapitre Paiement avec proposition au porteur de créer un alias à la page 109.

Tous droits réservés

11. UTILISER DES FONCTIONS COMPLÉMENTAIRES

Tous droits réservés

11.1. Définir un montant différent pour les n premières échéances

Vous souhaitez définir un abonnement dont la (ou les) première échéance est valorisée différemment de celles qui sont valorisées par le champ **vads_sub_amount**.

Exemple : définir un abonnement dont les 3 premières échéances sont à 45,25 EUR , et le reste des échéances à 75,90 EUR.

Pour cela :

1. Utilisez l'ensemble des champs nécessaires à votre cas d'utilisation (abonnement fixe) pour construire votre formulaire de paiement.

2. Utilisez les champs ci-dessous :

Nom du champ	Description	Valeur
vads_sub_init_amount_number	Nombre d'échéances auxquelles sera appliqué le montant défini par **vads_sub_init_amount**	3
vads_sub_init_amount	Montant des premières échéances. Le nombre des premières échéances est défini par **vads_sub_init_amount_number**	2500
vads_sub_amount	Montant des écheances de l'abonnement hormis celles éventuellement définies par **vads_sub_init_amount_number**	3000
vads_sub_currency	Devise utilisée pour l'ensemble des échéances de l'abonnement	Ex : 978 pour l'euro (EUR)

Les champs **vads_sub_init_amount** et **vads_sub_amount** ne peuvent pas être valorisés à 0.

Pour définir un abonnement dont les 3 premiers mois sont gratuits, il vous suffit de décaler la date d'effet (**vads_sub_effect_date**) de 3 mois.

Exemple de formulaire :

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_cust_country" value="FR" />
<input type="hidden" name="vads_cust_email" value="exemple@gmail.com" />
<input type="hidden" name="vads_cust_first_name" value="Paul" />
<input type="hidden" name="vads_cust_last_name" value="Juve" />
<input type="hidden" name="vads_cust_title" value="M." />
<input type="hidden" name="vads_page_action" value="REGISTER_SUBSCRIBE" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="91335531" />
<input type="hidden" name="vads_trans_date" value="20190716080441" />
<input type="hidden" name="vads_trans_id" value="362812" />
<input type="hidden" name="vads_validation_mode" value="0" />
<input type="hidden" name="vads_sub_currency" value="978" />
<input type="hidden" name="vads_sub_init_amount_number" value="3" />
<input type="hidden" name="vads_sub_init_amount" value="2500" />
<input type="hidden" name="vads_sub_amount" value="3000" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="G6oZchxNT+ySm7YQ/zvQvfgxmOmubvZ0lPwFKKVUSyI="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```


Tous droits réservés

11.2. Définir la devise pour la création ou la mise à jour d'un alias

Dans le cas où :

- vous possédez un contrat supportant plusieurs devises,
- vous possédez plusieurs boutiques,
- vos boutiques sont associées au même contrat,
- chaque boutique génère des paiements dans une devise différente,

  (ex: US dollar pour la première boutique, Euro pour la seconde boutique)

il est possible que la devise utilisée lors de la création ou la mise à jour d'un alias ne soit pas supportée par la boutique.

En effet, la plateforme de paiement sélectionne par défaut la première devise trouvée par ordre alphabétique pour réaliser les vérifications nécessaires auprès de l'émetteur du moyen de paiement.

Pour éviter des erreurs de traitement d'IPN, vous avez la possibilité de transmettre la devise à utiliser via le formulaire.

Il sera toujours possible d'utiliser l'alias pour réaliser des paiements dans n'importe quelle devise supportée par le contrat.

Nom du champ	Description	Format	Valeur
vads_currency	Code numérique de la monnaie à utiliser pour le paiement, selon la norme ISO 4217 (code numérique).	n3	Ex : 978 pour l'euro (EUR)

12. CALCULER LA SIGNATURE

Afin de pouvoir calculer la signature vous devez être en possession :

- de la totalité des champs dont le nom commence par `vads_`
- du type d'algorithme choisi dans la configuration de la boutique
- de la **clé**

La valeur de la clé est disponible dans votre Back Office Expert depuis le menu **Paramétrage** > **Boutique** > onglet **Clés**.

Le type d'algorithme est défini dans votre Back Office Expert depuis le menu **Paramétrage** > **Boutique** > onglet **Configuration**.

Pour un maximum de sécurité, il est recommandé d'utiliser l'algorithme HMAC-SHA-256 ainsi qu'une clé alphanumérique.

L'utilisation de l'algorithme SHA-1 est dépréciée mais maintenue pour des raisons de compatibilité.

Pour calculer la signature :

1. Triez les champs dont le nom commence par `vads_` par ordre alphabétique.
2. Assurez-vous que tous les champs soient encodés en UTF-8.
3. Concaténez les valeurs de ces champs en les séparant avec le caractère "**+**".
4. Concaténez le résultat avec la clé de test ou de production en les séparant avec le caractère "**+**".
5. Selon l'algorithme de signature défini dans la configuration de votre boutique:
   a. si votre boutique est configurée pour utiliser "SHA-1", appliquez la fonction de hachage **SHA-1** sur la chaîne obtenue à l'étape précédente. **Déprécié.**
   b. si votre boutique est configurée pour utiliser "HMAC-SHA-256", calculez et encodez au format Base64 la signature du message en utilisant l'algorithme **HMAC-SHA-256** avec les paramètres suivants:
      - la fonction de hachage SHA-256,
      - la clé de test ou de production (en fonction de la valeur du champ `vads_ctx_mode`) comme clé partagée,
      - le résultat de l'étape précédente comme message à authentifier.
6. Sauvegardez le résultat de l'étape précédente dans le champ `signature`.

Exemple de paramètres envoyés à la plateforme de paiement:

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_amount" value="5124" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20170129130025" />
<input type="hidden" name="vads_trans_id" value="123456" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="ycA5Do5tNvsnKdc/eP1bj2xa19z9q3iWPy9/rpesfS0="/>

<input type="submit" name="payer" value="Payer"/>
</form>
```

Cet exemple de formulaire s'analyse de la manière suivante:

1. On trie par ordre **alphabétique** les champs dont le nom commence par `vads_` :
   - vads_action_mode
   - vads_amount
   - vads_ctx_mode
   - vads_currency
   - vads_page_action
   - vads_payment_config
   - vads_site_id
   - vads_trans_date
   - vads_trans_id
   - vads_version
2. On concatène la valeur de ces champs avec le caractère "**+**" :

   ```
   INTERACTIVE+5124+TEST+978+PAYMENT+SINGLE+12345678+20170129130025+123456+V2
   ```

3. On ajoute la valeur de la clé de test à la fin de la chaîne en la séparant par le caractère "**+**". Dans cet exemple, la clé de test est **1122334455667788**

   ```
   INTERACTIVE+5124+TEST+978+PAYMENT+SINGLE+12345678+20170129130025+123456+V2+1122334455667788
   ```

4. Si vous utilisez l'algorithme SHA-1, appliquez-le à la chaîne obtenue.

   Le résultat à transmettre dans le champ `signature` est : **59c96b34c74b9375c332b0b6a32e6deeec87de2b**

5. Si votre boutique est configurée pour utiliser "HMAC-SHA-256", calculez et encodez au format Base64 la signature du message en utilisant l'algorithme **HMAC-SHA-256** avec les paramètres suivants:
   - la fonction de hachage SHA-256,
   - la clé de test ou de production (en fonction de la valeur du champ `vads_ctx_mode`) comme clé partagée,
   - le résultat de l'étape précédente comme message à authentifier.

   Le résultat à transmettre dans le champ `signature` est :

   ycA5Do5tNvsnKdc/eP1bj2xa19z9q3iWPy9/rpesfS0=

13. ENVOYER LA DEMANDE DE PAIEMENT

Pour finaliser un achat, l'acheteur doit être redirigé vers la page de paiement.

Son navigateur doit transmettre les données du formulaire de paiement.

13.1. Rediriger l'acheteur vers la page de paiement

L'URL de la plateforme de paiement est la suivante :

https://secure.lyra.com/vads-payment/

Exemple de paramètres envoyés à la plateforme de paiement:

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_amount" value="2990" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_cust_country" value="FR" />
<input type="hidden" name="vads_cust_email" value="me@example.com" />
<input type="hidden" name="vads_order_id" value="CMD012859" />
<input type="hidden" name="vads_page_action" value="REGISTER_PAY" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20200426101407" />
<input type="hidden" name="vads_trans_id" value="x6Z41p" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="NM25DPLKEbtGEHCDHn8MBT4ki6aJI/ODaWhCzCnAfvY="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

13.2. Gérer les erreurs

Si la plateforme détecte une anomalie lors de la réception du formulaire, un message d'erreur est affiché et l'acheteur ne peut pas procéder au paiement.

En mode test :

Le message indique l'origine de l'erreur et propose un lien vers la description du code erreur pour vous aider à identifier les causes possibles.

En mode production :

Le message indique à l'acheteur qu'un problème technique est survenu.

Dans les deux cas, le marchand reçoit un e-mail d'avertissement contenant :

- l'origine de l'erreur ;
- un lien vers les causes possibles pour ce code d'erreur pour faciliter le diagnostic ;
- l'ensemble des champs contenus dans le formulaire.

L'e-mail est envoyé au contact gestionnaire de l'enseigne.

Pour modifier cette adresse ou ajouter une adresse supplémentaire, contactez l'administration des ventes.

Vous avez aussi la possibilité de créer une règle de notification personnalisée pour recevoir cet e-mail sur une autre adresse.

Pour cela :

1. Connectez-vous à votre Back Office Expert.

https://secure.lyra.com/portal/

2. Ouvrez le menu **Paramétrage** > **Règles de notifications**.
3. Sélectionnez **Notification avancée**.
4. Sélectionnez le type de notification **E-mail envoyé au marchand**.
5. Cliquez sur **Suivant**.
6. Sélectionnez l'événement déclencheur **Formulaire de paiement invalide**.
7. Dans la section **Paramétrage général**, renseignez les champs :
   - **Libellé de la règle**
   - **Adresse e-mail à notifier**
8. Cliquez sur le bouton **Créer**.

Une description des codes d'erreur avec leurs causes possibles est disponible sur notre site :

https://docs.lyra.com/fr/collect/error-code/error-00.html

Durant le paiement, d'autres messages peuvent survenir.

Voici une liste des messages les plus courants:

Message	Description
Votre demande de paiement a été refusée par votre établissement financier.	• La banque de l'acheteur a refusé la demande d'autorisation ou de renseignement. • Les règles de gestion de risque ont provoqué le refus de la transaction.
Votre demande d'inscription a été refusée par votre établissement financier.	• La banque de l'acheteur a refusé la demande d'autorisation ou de renseignement. • Les règles de gestion de risque ont provoqué le refus de la transaction.
Cet ordre de paiement est expiré. Veuillez vous mettre en relation avec votre boutique	L'acheteur a cliqué sur le lien de paiement après la date de fin de validité de l'ordre.
Cet ordre de paiement a déjà été payé	L'acheteur a cliqué une nouvelle fois sur le lien de paiement après avoir déjà réalisé le paiement.
Un dysfonctionnement s'est produit lors de la demande de paiement, le site marchand a été informé de l'impossibilité de finaliser la transaction.	Le formulaire de paiement a été rejeté. Le responsable de la boutique a reçu un e-mail détaillant l'orgine de l'erreur.
La transaction a déjà été effectuée	Le site marchand envoie un identifiant de transaction déjà utilisé pour une autre transaction (acceptée ou refusée). L'identifiant de transaction doit être unique sur une journée (00:00:00 à 23:59:59 UTC).
Désolé, suite à une trop longue inactivité, vous avez été déconnecté.	• L'acheteur tente de valider son numéro de carte alors que sa session de paiement est expirée. La durée de session est de 10 minutes. • Le site marchand envoie un identifiant de transaction déjà utilisé mais n'ayant pas donné lieu à une transaction (paiement abandonné par exemple). L'identifiant de transaction doit être unique sur une journée (00:00:00 à 23:59:59 UTC).

Message	Description
Les cookies sont bloqués par votre navigateur. Veuillez les autoriser avant de relancer l'opération.	L'acheteur a désactivé l'utilisation des cookies dans son navigateur. Les cookies sont indispensables au bon déroulement du paiement.

14. IMPLÉMENTER L'IPN

Pour traiter le résultat des paiements, le site marchand doit disposer d'un script sur une page dédiée.

Cette page sera appelée automatiquement après chaque paiement (accepté ou refusé) : les paramètres liés au résultat du paiement sont envoyés en mode POST par la plateforme de paiement.

Cet appel serveur à serveur, synchrone au paiement, doit être le plus court possible et sa durée dépend uniquement de votre temps de traitement.

Le script doit comporter au moins les étapes ci-dessous:

- Récupérer la liste des champs présents dans la réponse envoyée en POST
- Calculer la signature en prenant en compte les données reçues
- Comparer la signature calculée avec celle réceptionnée
- Analyser la nature de la notification
- Récupérer le résultat du paiement

Le script peut par exemple tester l'état de la commande (ou l'information de votre choix) pour vérifier qu'elle n'ait pas déja été mise à jour.

Une fois ces étapes réalisées, le script peut mettre à jour la base de données (nouvel état de la commande, mise à jour du stock, enregistrement des informations du paiement etc.).

Afin de faciliter le support et le diagnostic par le marchand en cas d'erreur lors d'une notification, il est recommandé d'écrire des messages qui permettront de connaître à quel stade du traitement l'erreur s'est produite.

La plateforme lit et stocke les 256 premiers octets du corps de la réponse HTTP.

Vous pouvez écrire des messages tout au long du traitement. Voici un exemple de messages que vous pouvez utiliser:

Message	Cas d'usage
Data received	Message à afficher lors de la récupération des données. Permet de confirmer que la notification a bien été reçue par le site marchand.
POST is empty	Message à afficher lors de la récupération des données. Permet de mettre en évidence une éventuelle redirection qui aurait fait perdre les paramètres postés par la plateforme de paiement.
An error occurred while computing the signature.	Message à afficher lorsque la vérification de la signature de la réponse a échouée.
Order successfully updated.	Message à afficher à la fin du fichier une fois vos traitements terminés avec succès.
An error occurred while updating the order.	Message à afficher à la fin du fichier si une erreur s'est produite pendant vos traitements.

14.1. Préparer son environnement

Les notifications de type Appel URL de notification sont les plus importantes car elles représentent l'unique moyen fiable pour le site marchand d'obtenir le résultat d'un paiement.

Il est donc primordial de s'assurer du bon fonctionnement des notifications.

Voici quelques recommandations à suivre :

- Les notifications sont envoyées depuis une adresse IP comprise dans la plage **194.50.38.0/24**, port par défaut 443 (HTTPS) en mode Test et en mode Production. Il faut autoriser cette plage d'adresses d'IP en cas de restriction mise en place du côté du site marchand.
- Le marchand doit s'assurer que cette URL soit joignable par la plateforme de paiement sans redirection. Les redirections entraînent la perte des données présentes dans le POST.

  C'est le cas s'il existe une configuration sur vos équipements ou chez votre hébergeur qui redirige les URL de type "https://**www.**example.com" vers "https://example.com" ou "**http**://example.com" vers "**https**://example.com".

- La page ne doit pas comporter d'affichage HTML. L'accès aux ressources telles que les images ou feuilles de styles ralentissent les échanges entre la plateforme de paiement et le site marchand.

- Evitez au maximum d'intégrer des tâches consommatrices de temps comme la génération de facture PDF ou l'envoi d'e-mail dans votre script.

  Le temps de traitement influe directement sur le délai d'affichage de la page de résumé du paiement.

  Plus le traitement de la notification est long, plus l'affichage du ticket à l'acheteur est retardé.

  L'acheteur pourrait être tenté de fermer son navigateur et de repasser une commande.

  Au delà de 10s, la plateforme considère que l'appel a échoué (timeout).

- Assurez-vous que le temps de traitement de l'IPN soit le plus court possible (10s maximum). Ceci vous permettra :
  - d'apporter une expérience utilisateur fluide lors du paiement et augmenter les chances de conversion de paiement;
  - de fiabiliser la synchronisation du statut de la transaction dans votre SI afin que celui-ci soit conforme au résultat du paiement.

- Si votre page n'est accessible qu'en https, testez votre URL sur le site de Qualys SSL Labs (https://www.ssllabs.com/ssltest/ et modifiez votre configuration si nécessaire afin d'obtenir un grade A.

  Votre certificat SSL doit être signé par une autorité de certification connue et reconnue sur le marché.

- Assurez-vous d'utiliser les dernières versions du protocole TLS afin de maintenir un haut niveau de sécurité.

14.2. Récupérer les données retournées dans la réponse

Les données retournées dans la réponse dépendent des paramètres envoyés dans la demande de paiement, du type de paiement réalisé, des options de votre boutique et du format de la notification.

Les données sont toujours envoyées en **POST** par la plateforme de paiement.

La première étape consiste donc à récupérer le contenu reçu en mode POST.

Exemples :

- En PHP, les données seront stockées dans la superglobale **$_POST**.
- En ASP.NET (C#), vous devez utiliser la propriété **Form** de la classe **HttpRequest**.
- En java, vous devez utiliser la méthode **getParameter** de l'interface **HttpServletRequest**.

La réponse est constituée d'une liste de champs. Chaque champ contient une valeur réponse. La liste de champs peut être amenée à évoluer.

Le script devra effectuer une boucle pour récupérer la totalité des champs transmis.

Il est recommandé de tester la présence du champ **vads_hash**, présent uniquement lors d'une notification.

```
if (empty ($_POST)){
 echo 'POST is empty';

}else{
 echo 'Data Received ';
 if (isset($_POST['vads_hash'])){

  echo 'Form API notification detected';
  //Signature computation
  //Signature verification
  //Order Update
 }
}
```

14.3. Calculer la signature de l'IPN

La signature se calcule selon la même logique utilisée lors de la demande de paiement.

Les données transmises par la plateforme de paiement sont encodées en UTF-8. Toute altération des données reçues aboutira à un calcul de signature erroné.

Vous devez calculer la signature avec les champs reçus dans la notification et pas ceux que vous avez transmis dans la demande de paiement.

1. Prenez en considération la totalité des champs dont le nom commence par **vads_**.
2. Triez ces champs par ordre alphabétique.
3. Concaténez les valeurs de ces champs en les séparant avec le caractère "**+**".
4. Concaténez le résultat avec la clé de test ou de production en les séparant avec le caractère "**+**".
5. Selon l'algorithme de signature défini dans la configuration de votre boutique:
   a. si votre boutique est configurée pour utiliser "SHA-1", appliquez la fonction de hachage **SHA-1** sur la chaîne obtenue à l'étape précédente. **Déprécié.**
   b. si votre boutique est configurée pour utiliser "HMAC-SHA-256", calculez et encodez au format Base64 la signature du message en utilisant l'algorithme **HMAC-SHA-256** avec les paramètres suivants:
      - la fonction de hachage SHA-256,
      - la clé de test ou de production (en fonction de la valeur du champ `vads_ctx_mode`) comme clé partagée,
      - le résultat de l'étape précédente comme message à authentifier.

Exemples en PHP

```
function getSignature ($params,$key)
{
    /**
     * Fonction qui calcule la signature.
     * $params : tableau contenant les champs reçus dans l'IPN.
     * $key : clé de TEST ou de PRODUCTION
     */
    //Initialisation de la variable qui contiendra la chaine à chiffrer
    $contenu_signature = "";

    //Tri des champs par ordre alphabétique
    ksort($params);
    foreach($params as $nom=>$valeur){

        //Récupération des champs vads_
        if (substr($nom,0,5)=='vads_'){

            //Concaténation avec le séparateur "+"
            $contenu_signature .= $valeur."+";
         }
    }
    //Ajout de la clé en fin de chaine
    $contenu_signature .= $key;

    //Encodage base64 de la chaine chiffrée avec l'algorithme HMAC-SHA-256
    $sign = base64_encode(hash_hmac('sha256',$contenu_signature, $key, true));
    return $sign;
 }
```

14.4. Comparer les signatures

Pour s'assurer de l'intégrité de la réponse, vous devez comparer la signature contenue dans l'IPN avec la valeur calculée à l'étape précédente.

Il ne faut pas comparer la signature de l'IPN avec la signature que vous avez transmis dans votre demande de paiement.

Si les signatures correspondent,

- alors vous pouvez considérer la réponse comme sûre et procéder à la suite de l'analyse.
- sinon, le script devra lever une exception et avertir le marchand de l'anomalie.

Exemple PHP:

```
if ($_POST['signature'] == $sign){

    //Processing data

}else{
    throw new Exception('An error occurred while computing the signature');
}
```

Les signatures ne correspondent pas en cas :

- d'erreur d'implémentation (erreur dans votre calcul, problème d'encodage UTF-8, etc.),
- d'erreur dans la valeur de la clé utilisée ou dans celle du champ **vads_ctx_mode** (problème fréquent lors du passage en production),
- de tentative de corruption des données.

14.5. Analyser la nature de la notification

Le champ **vads_url_check_src** permet de différencier les notifications en fonction de leur évènement déclencheur :

- création d'un alias (avec ou sans souscription à un abonnement).
- paiement d'une échéance d'un abonnement.
- renvoi de la notification depuis le Back Office Expert par le marchand.

Il précise la règle de notification appliquée.

Valeurs associées au champ vads_url_check_src :

Valeur	Description
PAY	Création d'un paiement par formulaire. Valeur envoyée dans les cas suivants : • demande de création d'un mandat ou d'un alias (REGISTER) • demande de création d'un mandat ou d'un alias lors de la souscription à un abonnement (REGISTER_SUBSCRIBE) • paiement immédiat (paiement comptant ou première échéance d'un paiement en plusieurs fois) • paiement différé à moins de 7 jours • paiement abandonné ou annulé par l'acheteur uniquement si le marchand a configuré la règle "URL de notification sur annulation".
BO	Exécution de l'URL de notification depuis le Back Office Expert. (par clic droit sur une transaction > Exécuter l'URL de notification).
BATCH_AUTO	Valeur envoyée dans le cadre d'une demande d'autorisation sur un paiement qui était en attente d'autorisation. Non applicable pour le prélèvement ponctuel SEPA.
BATCH	Valeur envoyée dans le cas de la mise à jour du statut d'une transaction après synchronisation auprès de l'acquéreur. Uniquement si le marchand a configuré la règle "URL de notification sur modification par batch".
DCF	Valeur envoyée suite à une transaction provenant du formulaire de collecte de données.
MERCH_BO	Valeur envoyée suite à une opération réalisée depuis le Back Office Expert si le marchand a configuré la règle de notification : "URL de notification sur une opération provenant du Back Office".
PAYMENT_ORDER	Valeur envoyée suite à une transaction provenant d'un ordre de paiement (e-mail, URL de paiement ou SMS).
REC	Valeur envoyée uniquement pour les paiements par abonnement si le marchand a configuré la règle "URL de notification à la création d'un paiement récurrent". Non applicable pour le prélèvement ponctuel SEPA.
RETRY	Rejeu automatique de l'URL de notification.

En testant sa valeur, le script peut réaliser un traitement différent en fonction de la nature de la notification.

Par exemple :

Si **vads_url_check_src** est valorisé à **PAY** ou **BATCH_AUTO** alors le script met à jour le statut de la commande, ...

Si **vads_url_check_src** est valorisé à **REC** alors le script récupère la référence de l'abonnement et incrémente le nombre d'échéances échues en cas de paiement accepté, ...

Dans le cadre d'un prélèvement récurrent (issu d'un REGISTER_SUBSCRIBE), la plateforme de paiement notifie le créancier (marchand) lors de la création de chaque transaction.

14.6. Traiter les données de la réponse

- Création d'un alias sans paiement à la page 78
- Modification des informations associées à l'alias à la page 83
- Création de l'alias lors d'un paiement à la page 87
- Création de l'alias lors de la souscription à un abonnement à la page 92
- Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement à la page 97
- Paiement par alias à la page 102
- Souscription à un abonnement à la page 106
- Paiement avec proposition au porteur de créer un alias à la page 109
- Paiement d'une échéance d'un abonnement à la page 113

14.6.1. Création d'un alias sans paiement

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **REGISTER**.
vads_identifier_status	Statut de la création de alias. Les valeurs possibles sont : • **CREATED** : la demande d'autorisation ou de renseignement si l'acquéreur le supporte est acceptée. L'alias est créé avec succès et apparaît dans le Back Office Expert. • **NOT_CREATED** : la demande d'autorisation ou de renseignement est refusée. L'alias n'est pas créé. • **ABANDONED** : action abandonnée par l'acheteur. L'alias n'est pas créé.
vads_identifier	Identifiant de l'alias. La valeur retournée est : • soit identique à la valeur transmise dans la requête, quel que soit le résultat de la création de l'alias, même en cas d'abandon, • soit la valeur générée par la plateforme, si le champ n'est pas transmis dans la requête et que l'alias est bien créé (vads_identifier_status=CREATED). Le champ **vads_identifier** ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_identifier_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'alias n'est pas créé (vads_identifier_status=NOT_CREATED).
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur.

Tous droits réservés

Nom du champ	Description
	L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias. En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) l'identifiant de transaction émetteur sera utilisé comme référence de chaînage si nécessaire.
vads_cust_email	Adresse e-mail de l'acheteur transmise dans la requête.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Une demande de "création d'alias sans paiement" donne lieu à la création d'une transaction de type VERIFICATION, visible dans le Back Office Expert.

Le rôle de cette transaction est d'aider le marchand à comprendre, depuis son Back Office, les raisons du refus de la création de l'alias.

Voici ses caractéristiques :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **VERIFICATION**.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **ACCEPTED** La demande d'autorisation ou de renseignement a été acceptée. L'alias est créé et visible dans le Back Office Expert. • **REFUSED** La demande d'autorisation ou de renseignement a été refusée. L'alias n'est pas créé.
vads_occurrence_type	Type d'occurrence de la transaction. Sa valeur est **RECURRENT_INITIAL**.
vads_amount	Valeurs possibles : • **0** si l'acquéreur supporte les demandes de renseignements, • **100** dans le cas contraire.
vads_trans_id	Identifiant de la transaction. Sa valeur est générée par la plateforme de paiement.
vads_trans_uuid	Identifiant unique de la transaction. Sa valeur est générée par la plateforme de paiement.
vads_auth_mode	Type de demande réalisée auprès des serveurs d'autorisation. Sa valeur est **MARK**.
vads_auth_number	Numéro d'autorisation retourné par le serveur d'autorisation. Vide si autorisation échouée.

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les règles relatives au montant ou dont l'action est "Valider manuellement" ne s'appliquent pas dans le cas d'une transaction de type VERIFICATION.
Les valeurs possibles sont :
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>ENABLE_3DS</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>DISABLE_3DS</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>NO_PREFERENCE</td><td>• Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr>
<tr><td>NO_CHALLENGE_REQUEST</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.</td></tr>
<tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr>
<tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat.
Se référer à la description du champ vads_risk_analysis_result pour identifier la liste des valeurs possibles et leur description.</td></tr>
<tr><td>INFORM</td><td>• Une alerte est remontée.</td></tr>
</table>
</td></tr>
</table>

Tous droits réservés

Nom du champ	Description
	<table><tr><th>Valeurs</th><th>Description</th></tr><tr><td></td><td>• Le marchand est averti qu'un risque est identifié. • Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr></table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification du porteur :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible

Nom du champ	Remarque
	• **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

Tous droits réservés

14.6.2. Modification des informations associées à l'alias

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **REGISTER_UPDATE**.
vads_identifier_status	Statut de la mise à jour de alias. Les valeurs possibles sont : • **UPDATED** : l'alias a été mis à jour avec succès. • **NOT_UPDATED** : l'alias n'a pas été mis à jour. • **ABANDONED** : action abandonnée par l'acheteur. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert.
vads_identifier	Identifiant de l'alias à mettre à jour. La valeur retournée est identique à celle transmise dans la requête.
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur. L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias. En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) l'identifiant de transaction émetteur sera utilisé comme référence de chaînage si nécessaire.
vads_cust_email	Adresse e-mail de l'acheteur transmise dans la requête.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Une demande de "mise à jour d'alias" donne lieu à la création d'une transaction de type VERIFICATION, visible dans le Back Office Expert.

Le rôle de cette transaction est d'aider le marchand à comprendre, depuis son Back Office, les raisons du refus de la création de l'alias.

Voici ses caractéristiques :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **VERIFICATION**.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **ACCEPTED** La demande d'autorisation ou de renseignement a été acceptée. L'alias est créé et visible dans le Back Office Expert. • **REFUSED** La demande d'autorisation ou de renseignement a été refusée. L'alias n'est pas créé.

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td>vads_occurrence_type</td><td>Type d'occurrence de la transaction.
Sa valeur est RECURRENT_INITIAL.</td></tr>
<tr><td>vads_amount</td><td>Valeurs possibles :
0 si l'acquéreur supporte les demandes de renseignements,
100 dans le cas contraire.</td></tr>
<tr><td>vads_trans_id</td><td>Identifiant de la transaction.
Sa valeur est générée par la plateforme de paiement.</td></tr>
<tr><td>vads_trans_uuid</td><td>Identifiant unique de la transaction.
Sa valeur est générée par la plateforme de paiement.</td></tr>
<tr><td>vads_auth_mode</td><td>Type de demande réalisée auprès des serveurs d'autorisation.
Sa valeur est MARK.</td></tr>
<tr><td>vads_auth_number</td><td>Numéro d'autorisation retourné par le serveur d'autorisation.
Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les règles relatives au montant ou dont l'action est "Valider manuellement" ne s'appliquent pas dans le cas d'une transaction de type VERIFICATION.
Les valeurs possibles sont :
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>ENABLE_3DS</td><td>Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>DISABLE_3DS</td><td>Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>NO_PREFERENCE</td><td>Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr>
<tr><td>NO_CHALLENGE_REQUEST</td><td>Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.</td></tr>
<tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr>
<tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat.
Se référer à la description du champ vads_risk_analysis_result pour identifier la liste des valeurs possibles et leur description.</td></tr>
<tr><td>INFORM</td><td>• Une alerte est remontée.
• Le marchand est averti qu’un risque est identifié.
• Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr>
</table>
</td></tr>
</table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d’un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d’expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Nom du champ	Remarque
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification du porteur :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

Tous droits réservés

14.6.3. Création de l'alias lors d'un paiement

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **REGISTER_PAY**.
vads_identifier_status	Statut de la création de alias. Les valeurs possibles sont : • **CREATED** : la demande d'autorisation ou de renseignement si l'acquéreur le supporte est acceptée. L'alias est créé avec succès. • **NOT_CREATED** : la demande d'autorisation ou de renseignement est refusée. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert. • **ABANDONED** : action abandonnée par l'acheteur. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **AUTHORISED** La demande d'autorisation ou de renseignement a été acceptée. L'alias est créé et visible dans le Back Office Expert. • **AUTHORISED_TO_VALIDATE** La demande d'autorisation ou de renseignement a été acceptée. Le marchand doit valider manuellement la transaction. L'alias est créé et visible dans le Back Office Expert. • **CAPTURED** La demande d'autorisation ou de renseignement a été acceptée. Le paiement est visible dans l'onglet "Transactions remisées" du Back Office. L'alias est créé et visible dans le Back Office Expert. • **WAITING_AUTHORISATION** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. La demande d'autorisation pour le montant total n'a pas encore eu lieu. L'alias est créé et visible dans le Back Office Expert. • **WAITING_AUTHORISATION_TO_VALIDATE** **A valider et autoriser** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. Une autorisation 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte) a été acceptée. Le marchand doit valider manuellement la transaction afin de déclencher la demande d'autorisation et la capture. • **REFUSED** La demande d'autorisation ou de renseignement a été refusée. L'alias n'est pas créé. • **ABANDONED** Opération abandonnée par l'acheteur. La transaction n'apparaît pas dans le Back Office Expert. L'alias n'est pas créé.

Tous droits réservés

Nom du champ	Description
vads_identifier	Identifiant de l'alias. La valeur retournée est : • soit identique à la valeur transmise dans la requête, quel que soit le résultat de la création de l'alias, même en cas d'abandon, • soit la valeur générée par la plateforme, si le champ n'est pas transmis dans la requête et que l'alias est bien créé (vads_identifier_status=CREATED). Le champ **vads_identifier** ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_identifier_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'alias n'est pas créé (vads_identifier_status=NOT_CREATED).
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur. • L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias et de la transaction. En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) l'identifiant de transaction émetteur sera utilisé comme référence de chaînage si nécessaire. • Dans le cas où le marchand duplique (MIT) la transaction, la plateforme utilisera automatiquement cet identifiant comme référence de chaînage.
vads_cust_email	Adresse e-mail de l'acheteur transmise dans la requête.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Pour connaître le détail du paiement consultez les paramètres ci-dessous :

Informations sur la transaction :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **DEBIT**.
vads_occurrence_type	Type d'occurrence de la transaction. Sa valeur est **RECURRENT_INITIAL**.
vads_amount	Montant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_currency	Code de la devise utilisée pour le paiement.
vads_trans_id	Identifiant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_trans_uuid	Identifiant unique de la transaction.

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>Sa valeur est générée par la plateforme de paiement.</td></tr>
<tr><td>vads_contract_used</td><td>Numéro du contrat associé à la transaction.</td></tr>
<tr><td>vads_auth_mode</td><td>Type de demande réalisée auprès des serveurs d'autorisation:
MARK : correspond à une autorisation de 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte).
Valeur utilisée également si la durée séparant la date de remise demandée de la date du jour est strictement supérieure à la durée de validité de l'autorisation.
FULL : correspond à une autorisation du montant total de la transaction.
Valeur utilisée si la durée séparant la date de remise demandée de la date du jour est strictement inférieure à la durée de validité de l'autorisation.</td></tr>
<tr><td>vads_auth_number</td><td>Numéro d'autorisation retourné par le serveur d'autorisation.
Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_control</td><td>Résultat des contrôles de risque.
Lorsque qu'au moins un contrôle retourne la valeur ERROR, la transaction est refusée.
Consultez la description du champ vads_risk_analysis_result pour plus de détails.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les valeurs possibles sont :<table><tr><th>Valeurs</th><th>Description</th></tr><tr><td>ENABLE_3DS</td><td>Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr><tr><td>DISABLE_3DS</td><td>Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr><tr><td>NO_PREFERENCE</td><td>Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr><tr><td>NO_CHALLENGE_REQUEST</td><td>Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr><tr><td>CHALLENGE_REQUESTED</td><td>Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr><tr><td>CHALLENGE_MANDATE</td><td>Le module de risque a demandé une authentification avec interaction du</td></tr></table></td></tr>
</table>

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td></td><td>porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.</td></tr>
<tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr>
<tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat.
Se référer à la description du champ vads_risk_analysis_result pour identifier la liste des valeurs possibles et leur description.</td></tr>
<tr><td>INFORM</td><td>• Une alerte est remontée.
• Le marchand est averti qu’un risque est identifié.
• Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr>
</table>
</td></tr>
</table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d’un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d’expiration de la carte utilisée.

Nom du champ	Remarque
	Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification du porteur :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

Tous droits réservés

14.6.4. Création de l'alias lors de la souscription à un abonnement

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **REGISTER_SUBSCRIBE**.
vads_identifier_status	Statut de la création de alias. Les valeurs possibles sont : • **CREATED** : la demande d'autorisation ou de renseignement si l'acquéreur le supporte est acceptée. L'alias est créé avec succès. Consultez la valeur du champ vads_recurrence_status pour déterminer si l'abonnement est créé. • **NOT_CREATED** : la demande d'autorisation ou de renseignement est refusée. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert. L'abonnement n'est pas créé. • **ABANDONED** : action abandonnée par l'acheteur. L'alias n'est pas créé et n'apparaîtra pas dans le Back Office Expert. L'abonnement n'est pas créé.
vads_recurrence_status	Statut de la création de l'abonnement. Les valeurs possibles sont: • **CREATED**: L'abonnement est créé avec succès. • **NOT_CREATED**: L'abonnement n'est pas créé. • **ABANDONED**: action abandonnée par l'acheteur. L'abonnement n'est pas créé.
vads_identifier	Identifiant de l'alias. La valeur retournée est : • soit identique à la valeur transmise dans la requête, quel que soit le résultat de la création de l'alias, même en cas d'abandon, • soit la valeur générée par la plateforme, si le champ n'est pas transmis dans la requête et que l'alias est bien créé (vads_identifier_status=CREATED). Le champ **vads_identifier** ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_identifier_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'alias n'est pas créé (vads_identifier_status=NOT_CREATED).
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur. L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias. En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) l'identifiant de transaction émetteur sera utilisé comme référence de chaînage si nécessaire.
vads_cust_email	Adresse e-mail de l'acheteur transmise dans la requête.

Nom du champ	Description
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Pour connaître le détail de l'abonnement consultez les paramètres ci-dessous :

Nom du champ	Remarque
vads_subscription	Identifiant de l'abonnement. La valeur retournée est : • soit la valeur transmise dans la requête, quel que soit le résultat de la création de l'abonnement, • soit la valeur de générée par la plateforme de paiement, si le champ n'est pas transmis dans la requête et que l'abonnement est créé avec succès (vads_recurrence_status=CREATED). Le champ vads_subscription ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_recurrence_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'abonnement n'est pas créé (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Montant des échéances de l'abonnement (dans sa plus petite fraction monétaire).
vads_sub_currency	Code de la devise utilisée pour l'abonnement. Ex : 978 pour l'euro (EUR)
vads_sub_desc	Règle de récurrence à appliquer suivant la spécification iCalendar RFC5545. Ex : RRULE:FREQ=MONTHLY
vads_sub_effect_date	Date de début de l'abonnement (ou date d'effet) dans le fuseau UTC, au format AAAAMMJJ. Ex : 20210601
vads_sub_init_amount	Montant des premières échéances. Le nombre des premières échéances est défini par **vads_sub_init_amount_number**. Ex : 1000
vads_sub_init_amount_number	Nombre d'échéances auxquelles sera appliqué le montant défini par **vads_sub_init_amount**. Ex : 3

Une demande de "création d'alias lors de la souscription d'un abonnement" donne lieu à la création d'une transaction de type VERIFICATION, visible dans le Back Office Expert.

Le rôle de cette transaction est d'aider le marchand à comprendre, depuis son Back Office, les raisons du refus de la création de l'alias.

Voici ses caractéristiques :

Nom du champ	Description
vads_operation_type	Type de transaction.

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>Sa valeur est VERIFICATION.</td></tr>
<tr><td>vads_trans_status</td><td>Statut de la transaction.
Les valeurs possibles sont :
ACCEPTED
La demande d'autorisation ou de renseignement a été acceptée.
L'alias est créé et visible dans le Back Office Expert.
REFUSED
La demande d'autorisation ou de renseignement a été refusée.
L'alias n'est pas créé.</td></tr>
<tr><td>vads_occurrence_type</td><td>Type d'occurrence de la transaction.
Sa valeur est RECURRENT_INITIAL.</td></tr>
<tr><td>vads_amount</td><td>Valeurs possibles :
0 si l'acquéreur supporte les demandes de renseignements,
100 dans le cas contraire.</td></tr>
<tr><td>vads_trans_id</td><td>Identifiant de la transaction.
Sa valeur est générée par la plateforme de paiement.</td></tr>
<tr><td>vads_trans_uuid</td><td>Identifiant unique de la transaction.
Sa valeur est générée par la plateforme de paiement.</td></tr>
<tr><td>vads_auth_mode</td><td>Type de demande réalisée auprès des serveurs d'autorisation.
Sa valeur est MARK.</td></tr>
<tr><td>vads_auth_number</td><td>Numéro d'autorisation retourné par le serveur d'autorisation.
Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les règles relatives au montant ou dont l'action est "Valider manuellement" ne s'appliquent pas dans le cas d'une transaction de type VERIFICATION.
Les valeurs possibles sont :<table><tr><th>Valeurs</th><th>Description</th></tr><tr><td>ENABLE_3DS</td><td>Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr><tr><td>DISABLE_3DS</td><td>Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr><tr><td>NO_PREFERENCE</td><td>Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr></table></td></tr>
</table>

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>NO_CHALLENGE_REQUEST</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.</td></tr>
<tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr>
<tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat.
Se référer à la description du champ vads_risk_analysis_result pour identifier la liste des valeurs possibles et leur description.</td></tr>
<tr><td>INFORM</td><td>• Une alerte est remontée.
• Le marchand est averti qu’un risque est identifié.
• Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr>
</table>
</td></tr>
</table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.

Nom du champ	Remarque
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification du porteur :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

Tous droits réservés

14.6.5. Création de l'alias lors de la souscription d'un abonnement accompagné d'un paiement

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **REGISTER_PAY_SUBSCRIBE**.
vads_identifier_status	Statut de la création de alias. Les valeurs possibles sont : • **CREATED** : la demande d'autorisation ou de renseignement si l'acquéreur le supporte est acceptée. L'alias est créé avec succès. Consultez la valeur du champ vads_recurrence_status pour déterminer si l'abonnement est créé. • **NOT_CREATED** : la demande d'autorisation ou de renseignement est refusée. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert. L'abonnement n'est pas créé. • **ABANDONED** : action abandonnée par l'acheteur. L'alias n'est pas créé et n'apparaîtra pas dans le Back Office Expert. L'abonnement n'est pas créé.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **AUTHORISED** La demande d'autorisation ou de renseignement a été acceptée. L'alias est créé et visible dans le Back Office Expert. • **AUTHORISED_TO_VALIDATE** La demande d'autorisation ou de renseignement a été acceptée. Le marchand doit valider manuellement la transaction. L'alias est créé et visible dans le Back Office Expert. • **CAPTURED** La demande d'autorisation ou de renseignement a été acceptée. Le paiement est visible dans l'onglet "Transactions remisées" du Back Office. L'alias est créé et visible dans le Back Office Expert. • **WAITING_AUTHORISATION** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. La demande d'autorisation pour le montant total n'a pas encore eu lieu. L'alias est créé et visible dans le Back Office Expert. • **WAITING_AUTHORISATION_TO_VALIDATE** **A valider et autoriser** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. Une autorisation 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte) a été acceptée. Le marchand doit valider manuellement la transaction afin de déclencher la demande d'autorisation et la capture. • **REFUSED** La demande d'autorisation ou de renseignement a été refusée. L'alias n'est pas créé.

Nom du champ	Description
	• **ABANDONED** Opération abandonnée par l'acheteur. La transaction n'apparaît pas dans le Back Office Expert. L'alias n'est pas créé.
vads_recurrence_status	Statut de la création de l'abonnement. Les valeurs possibles sont : • **CREATED** : L'abonnement est créé avec succès. • **NOT_CREATED** : L'abonnement n'est pas créé. • **ABANDONED** : action abandonnée par l'acheteur. L'abonnement n'est pas créé.
vads_identifier	Identifiant de l'alias. La valeur retournée est : • soit identique à la valeur transmise dans la requête, quel que soit le résultat de la création de l'alias, même en cas d'abandon, • soit la valeur générée par la plateforme, si le champ n'est pas transmis dans la requête et que l'alias est bien créé (vads_identifier_status=CREATED). Le champ **vads_identifier** ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_identifier_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'alias n'est pas créé (vads_identifier_status=NOT_CREATED).
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur. L'identifiant de transaction émetteur est stocké par la plateforme de paiement au niveau de l'alias et de la transaction. En fonction de l'utilisation que vous ferez de l'alias (paiement 1 clic, paiement 0 clic, abonnement, etc.) l'identifiant de transaction émetteur sera utilisé comme référence de chaînage si nécessaire.
vads_cust_email	Adresse e-mail de l'acheteur transmise dans la requête.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Pour connaître le détail de l'abonnement consultez les paramètres ci-dessous :

Nom du champ	Remarque
vads_subscription	Identifiant de l'abonnement. La valeur retournée est : • soit la valeur transmise dans la requête, quel que soit le résultat de la création de l'abonnement,

Nom du champ	Remarque
	• soit la valeur de générée par la plateforme de paiement, si le champ n'est pas transmis dans la requête et que l'abonnement est créé avec succès (vads_recurrence_status=CREATED). Le champ vads_subscription ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_recurrence_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'abonnement n'est pas créé (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Montant des échéances de l'abonnement (dans sa plus petite fraction monétaire).
vads_sub_currency	Code de la devise utilisée pour l'abonnement. Ex : 978 pour l'euro (EUR)
vads_sub_desc	Règle de récurrence à appliquer suivant la spécification iCalendar RFC5545. Ex : RRULE:FREQ=MONTHLY
vads_sub_effect_date	Date de début de l'abonnement (ou date d'effet) dans le fuseau UTC, au format AAAAMMJJ. Ex : 20210601
vads_sub_init_amount	Montant des premières échéances. Le nombre des premières échéances est défini par **vads_sub_init_amount_number**. Ex : 1000
vads_sub_init_amount_number	Nombre d'échéances auxquelles sera appliqué le montant défini par **vads_sub_init_amount**. Ex : 3

Pour connaître le détail du paiement consultez les paramètres ci-dessous :

Informations sur la transaction :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **DEBIT**.
vads_occurrence_type	Type d'occurrence de la transaction. Sa valeur est **RECURRENT_INITIAL**.
vads_amount	Montant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_currency	Code de la devise utilisée pour le paiement.
vads_trans_id	Identifiant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_trans_uuid	Identifiant unique de la transaction. Sa valeur est générée par la plateforme de paiement.
vads_contract_used	Numéro du contrat associé à la transaction.
vads_auth_mode	Type de demande réalisée auprès des serveurs d'autorisation: • **MARK** : correspond à une autorisation de 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte).

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>Valeur utilisée également si la durée séparant la date de remise demandée de la date du jour est strictement supérieure à la durée de validité de l'autorisation.
• FULL : correspond à une autorisation du montant total de la transaction.
Valeur utilisée si la durée séparant la date de remise demandée de la date du jour est strictement inférieure à la durée de validité de l'autorisation.</td></tr>
<tr><td>vads_auth_number</td><td>Numéro d'autorisation retourné par le serveur d'autorisation.
Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_control</td><td>Résultat des contrôles de risque.
Lorsque qu'au moins un contrôle retourne la valeur ERROR, la transaction est refusée.
Consultez la description du champ vads_risk_analysis_result pour plus de détails.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les valeurs possibles sont :
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>ENABLE_3DS</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>DISABLE_3DS</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>NO_PREFERENCE</td><td>• Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr>
<tr><td>NO_CHALLENGE_REQUES</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au</td></tr>
</table></td></tr>
</table>

Nom du champ	Description
	<table><tr><th>Valeurs</th><th>Description</th></tr><tr><td></td><td>marchand de procéder à toutes les vérifications souhaitées.</td></tr><tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr><tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat. Se référer à la description du champ **vads_risk_analysis_result** pour identifier la liste des valeurs possibles et leur description.</td></tr><tr><td>INFORM</td><td>• Une alerte est remontée. • Le marchand est averti qu'un risque est identifié. • Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr></table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification du porteur :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

14.6.6. Paiement par alias

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **PAYMENT**.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **AUTHORISED** La demande d'autorisation a été acceptée. • **AUTHORISED_TO_VALIDATE** La demande d'autorisation a été acceptée. Le marchand doit valider manuellement la transaction. • **CAPTURED** La demande d'autorisation a été acceptée. Le paiement est visible dans l'onglet "Transactions remisées" du Back Office. • **WAITING_AUTHORISATION**

Nom du champ	Description
	Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. La demande d'autorisation pour le montant total n'a pas encore eu lieu. • **WAITING_AUTHORISATION_TO_VALIDATE** **A valider et autoriser** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. Une autorisation 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte) a été acceptée. Le marchand doit valider manuellement la transaction afin de déclencher la demande d'autorisation et la capture. • **REFUSED** La demande d'autorisation a été refusée. • **ABANDONED** Opération abandonnée par l'acheteur. La transaction n'apparaît pas dans le Back Office Expert.
vads_identifier	Identifiant de l'alias à débiter. La valeur retournée est identique à celle transmise dans la requête.
vads_cust_email	Adresse e-mail de l'acheteur associé à l'alias.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Pour connaître le détail du paiement consultez les paramètres ci-dessous :

Informations sur la transaction :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **DEBIT**.
vads_occurrence_type	Type d'occurrence de la transaction. Sa valeur est **RECURRENT_INTERMEDIAIRE**.
vads_amount	Montant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_currency	Code de la devise utilisée pour le paiement.
vads_trans_id	Identifiant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_trans_uuid	Identifiant unique de la transaction. Sa valeur est générée par la plateforme de paiement.
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur.
vads_contract_used	Numéro du contrat associé à la transaction.
vads_auth_mode	Type de demande réalisée auprès des serveurs d'autorisation : • **MARK** : correspond à une autorisation de 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte).

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>Valeur utilisée également si la durée séparant la date de remise demandée de la date du jour est strictement supérieure à la durée de validité de l'autorisation.
• FULL : correspond à une autorisation du montant total de la transaction.
Valeur utilisée si la durée séparant la date de remise demandée de la date du jour est strictement inférieure à la durée de validité de l'autorisation.</td></tr>
<tr><td>vads_auth_number</td><td>Numéro d'autorisation retourné par le serveur d'autorisation.
Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_control</td><td>Résultat des contrôles de risque.
Lorsque qu'au moins un contrôle retourne la valeur ERROR, la transaction est refusée.
Consultez la description du champ vads_risk_analysis_result pour plus de détails.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les valeurs possibles sont :
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>ENABLE_3DS</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>DISABLE_3DS</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>NO_PREFERENCE</td><td>• Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr>
<tr><td>NO_CHALLENGE_REQUE</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au</td></tr>
</table></td></tr>
</table>

Nom du champ	Description
	<table><tr><th>Valeurs</th><th>Description</th></tr><tr><td></td><td>marchand de procéder à toutes les vérifications souhaitées.</td></tr><tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr><tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat. Se référer à la description du champ **vads_risk_analysis_result** pour identifier la liste des valeurs possibles et leur description.</td></tr><tr><td>INFORM</td><td>• Une alerte est remontée. • Le marchand est averti qu'un risque est identifié. • Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr></table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification forte :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Les valeurs possibles sont : • "Vide" si l'acheteur ne s'est pas authentifié correctement, • **FRICTIONLESS** : authentification du porteur sans interaction avec l'ACS. Valeur retournée uniquement en 3DS v2, • **CHALLENGE** : authentification interactive du porteur (saisie OTP ou réponse à une série de questions). Valeur retournée en 3DS v1 et 3DS v2.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide: Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide: Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

14.6.7. Souscription à un abonnement

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **SUBSCRIBE**.
vads_recurrence_status	Statut de la création de l'abonnement. Les valeurs possibles sont: • **CREATED** : L'abonnement est créé avec succès. • **NOT_CREATED** : L'abonnement n'est pas créé. • **ABANDONED** : action abandonnée par l'acheteur. L'abonnement n'est pas créé.
vads_identifier	Identifiant de l'alias à débiter. La valeur retournée est identique à celle transmise dans la requête.

Nom du champ	Description
vads_cust_email	Adresse e-mail de l'acheteur associée à l'alias.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Pour connaître le détail de l'abonnement consultez les paramètres ci-dessous :

Nom du champ	Remarque
vads_subscription	Identifiant de l'abonnement. La valeur retournée est : • soit la valeur transmise dans la requête, quel que soit le résultat de la création de l'abonnement, • soit la valeur de générée par la plateforme de paiement, si le champ n'est pas transmis dans la requête et que l'abonnement est créé avec succès (vads_recurrence_status=CREATED). Le champ vads_subscription ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_recurrence_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'abonnement n'est pas créé (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Montant des échéances de l'abonnement (dans sa plus petite fraction monétaire).
vads_sub_currency	Code de la devise utilisée pour l'abonnement. Ex : 978 pour l'euro (EUR)
vads_sub_desc	Règle de récurrence à appliquer suivant la spécification iCalendar RFC5545. Ex : RRULE:FREQ=MONTHLY
vads_sub_effect_date	Date de début de l'abonnement (ou date d'effet) dans le fuseau UTC, au format AAAAMMJJ. Ex : 20210601
vads_sub_init_amount	Montant des premières échéances. Le nombre des premières échéances est défini par **vads_sub_init_amount_number**. Ex : 1000
vads_sub_init_amount_number	Nombre d'échéances auxquelles sera appliqué le montant défini par **vads_sub_init_amount**. Ex : 3

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.

Nom du champ	Remarque
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification forte réalisée lors de la création de l'alias :

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

Tous droits réservés

14.6.8. Paiement avec proposition au porteur de créer un alias

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **ASK_REGISTER_PAY**.
vads_identifier_status	Statut de la création de alias. **Le champ ne sera pas envoyé si l'acheteur n'a pas donné son accord pour l'enregistrement de ses données de carte**. Les valeurs possibles sont : • **CREATED** : la demande d'autorisation ou de renseignement si l'acquéreur le supporte est acceptée. L'alias est créé avec succès. • **NOT_CREATED** : la demande d'autorisation ou de renseignement est refusée. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert. • **ABANDONED** : action abandonnée par l'acheteur. L'alias n'est pas créé et n'apparaît pas dans le Back Office Expert.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **AUTHORISED** La demande d'autorisation ou de renseignement a été acceptée. L'alias est créé et visible dans le Back Office Expert. • **AUTHORISED_TO_VALIDATE** La demande d'autorisation ou de renseignement a été acceptée. Le marchand doit valider manuellement la transaction. L'alias est créé et visible dans le Back Office Expert. • **CAPTURED** La demande d'autorisation ou de renseignement a été acceptée. Le paiement est visible dans l'onglet "Transactions remisées" du Back Office. L'alias est créé et visible dans le Back Office Expert. • **WAITING_AUTHORISATION** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. La demande d'autorisation pour le montant total n'a pas encore eu lieu. L'alias est créé et visible dans le Back Office Expert. • **WAITING_AUTHORISATION_TO_VALIDATE** **A valider et autoriser** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation. Une autorisation 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte) a été acceptée. Le marchand doit valider manuellement la transaction afin de déclencher la demande d'autorisation et la remise en banque. • **REFUSED** La demande d'autorisation ou de renseignement a été refusée. L'alias n'est pas créé. • **ABANDONED** Opération abandonnée par l'acheteur.

Nom du champ	Description
	La transaction n'apparaît pas dans le Back Office Expert. L'alias n'est pas créé.
vads_identifier	Identifiant de l'alias. **Le champ ne sera pas envoyé si l'acheteur n'a pas donné son accord pour l'enregistrement de ses données de carte**. La valeur retournée est : • soit identique à la valeur transmise dans la requête, quel que soit le résultat de la création de l'alias, même en cas d'abandon, • soit la valeur générée par la plateforme, si le champ n'est pas transmis dans la requête et que l'alias est bien créé (vads_identifier_status=CREATED). Le champ **vads_identifier** ne sera pas retourné : • s'il n'est pas transmis dans la requête et que l'acheteur abandonne (vads_identifier_status=ABANDONED), • s'il n'est pas transmis dans la requête et que l'alias n'est pas créé (vads_identifier_status=NOT_CREATED).
vads_cust_email	Adresse e-mail de l'acheteur transmise dans la requête.
vads_site_id	Identifiant de la boutique. La valeur retournée est identique à celle transmise dans la requête.
vads_ctx_mode	Mode de fonctionnement. La valeur retournée (**TEST** ou **PRODUCTION**) est identique à celle transmise dans la requête.

Pour connaître le détail du paiement consultez les paramètres ci-dessous :

Informations sur la transaction :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **DEBIT**.
vads_amount	Montant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_currency	Code de la devise utilisée pour le paiement.
vads_trans_id	Identifiant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_trans_uuid	Identifiant unique de la transaction. Sa valeur est générée par la plateforme de paiement.
vads_initial_issuer_transaction_identifier	Identifiant de transaction unique généré par l'émetteur.
vads_contract_used	Numéro du contrat associé à la transaction.
vads_auth_mode	Type de demande réalisée auprès des serveurs d'autorisation: • **MARK** : correspond à une autorisation de 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte). Valeur utilisée également si la durée séparant la date de remise demandée de la date du jour est strictement supérieure à la durée de validité de l'autorisation.

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>• FULL : correspond à une autorisation du montant total de la transaction.
Valeur utilisée si la durée séparant la date de remise demandée de la date du jour est strictement inférieure à la durée de validité de l'autorisation.</td></tr>
<tr><td>vads_auth_number</td><td>Numéro d'autorisation retourné par le serveur d'autorisation.
Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_control</td><td>Résultat des contrôles de risque.
Lorsque qu'au moins un contrôle retourne la valeur ERROR, la transaction est refusée.
Consultez la description du champ vads_risk_analysis_result pour plus de détails.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les valeurs possibles sont :
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>ENABLE_3DS</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>DISABLE_3DS</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>NO_PREFERENCE</td><td>• Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr>
<tr><td>NO_CHALLENGE_REQUES</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.</td></tr>
</table></td></tr>
</table>

Nom du champ	Description
	<table><tr><th>Valeurs</th><th>Description</th></tr><tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr><tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat. Se référer à la description du champ **vads_risk_analysis_result** pour identifier la liste des valeurs possibles et leur description.</td></tr><tr><td>INFORM</td><td>• Une alerte est remontée. • Le marchand est averti qu'un risque est identifié. • Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).</td></tr></table>

Informations sur le moyen de paiement utilisé :

Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Détails de l'authentification du porteur :

Tous droits réservés

Nom du champ	Remarque
vads_threeds_auth_type	Type d'authentification du porteur. Une authentification forte du porteur est obligatoire lors de l'enregistrement d'une carte. Le champ sera donc toujours valorisé à **CHALLENGE**.
vads_threeds_enrolled	Statut de l'inscription du porteur au programme 3D Secure. Les valeurs possibles sont : • **Y** : Authentification disponible. • **N** : Authentification non disponible • **U** : Statut de l'inscription au programme 3DS inconnu • vide : Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non inscrit ou moyen de paiement non éligible au 3DS).
vads_threeds_status	Résultat de l'authentification 3D Secure. Les valeurs possibles sont : • **Y** : Porteur authentifié avec succès. • **N** : Erreur d'authentification du porteur. • **U** : Authentification impossible • **A** : Tentative d'authentification mais authentification non réalisée. • vide : Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non inscrit ou moyen de paiement non éligible au 3DS).

Les champs facultatifs transmis dans la requête sont retournés dans la réponse sans modification de leur valeur.

14.6.9. Paiement d'une échéance d'un abonnement

Pour comprendre le résultat, analysez les champs ci-dessous :

Nom du champ	Description
vads_page_action	Action réalisée. La valeur retournée est **PAYMENT**.
vads_trans_status	Statut de la transaction. Les valeurs possibles sont : • **AUTHORISED** La demande d'autorisation a été acceptée. • **AUTHORISED_TO_VALIDATE** La demande d'autorisation a été acceptée. Le marchand doit valider manuellement la transaction. • **CAPTURED** La demande d'autorisation a été acceptée. Le paiement est visible dans l'onglet "Transactions remisées" du Back Office. • **REFUSED** La demande d'autorisation a été refusée.
vads_identifier	Identifiant de l'alias.

Nom du champ	Description
vads_cust_email	Adresse e-mail de l'acheteur.
vads_site_id	Identifiant de la boutique.
vads_ctx_mode	Mode de fonctionnement.

Pour connaître le détail de l'abonnement consultez les paramètres ci-dessous :

Nom du champ	Remarque
vads_subscription	Identifiant de l'abonnement.
vads_recurrence_number	Numéro de l'échéance de l'abonnement.

Pour connaître le détail du paiement consultez les paramètres ci-dessous :

Informations sur la transaction :

Nom du champ	Description
vads_operation_type	Type de transaction. Sa valeur est **DEBIT**.
vads_occurrence_type	Type d'occurrence de la transaction. Valeurs possibles : • **RECURRENT_INITIAL** : Première échéance. • **RECURRENT_INTERMEDIAIRE** : Énième échéance. Consultez le champ **vads_recurrence_number** pour connaître le numéro de l'échéance. • **RECURRENT_FINAL** : Dernière échéance.
vads_amount	Montant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_currency	Code de la devise utilisée pour le paiement.
vads_trans_id	Identifiant de la transaction. La valeur retournée est identique à celle transmise dans la requête.
vads_trans_uuid	Identifiant unique de la transaction. Sa valeur est générée par la plateforme de paiement.
vads_contract_used	Numéro du contrat associé à la transaction.
vads_auth_mode	Type de demande réalisée auprès des serveurs d'autorisation: • **MARK** : correspond à une autorisation de 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte). Valeur utilisée également si la durée séparant la date de remise demandée de la date du jour est strictement supérieure à la durée de validité de l'autorisation. • **FULL** : correspond à une autorisation du montant total de la transaction. Valeur utilisée si la durée séparant la date de remise demandée de la date du jour est strictement inférieure à la durée de validité de l'autorisation.
vads_auth_number	Numéro d'autorisation retourné par le serveur d'autorisation.

<table>
<tr><th>Nom du champ</th><th>Description</th></tr>
<tr><td></td><td>Vide si autorisation échouée.</td></tr>
<tr><td>vads_auth_result</td><td>Code retour de la demande d'autorisation retournée par la banque émettrice.
Voir chapitre Gérer les codes retour de la demande d'autorisation.
Vide si erreur avant autorisation.</td></tr>
<tr><td>vads_risk_control</td><td>Résultat des contrôles de risque.
Lorsque qu'au moins un contrôle retourne la valeur ERROR, la transaction est refusée.
Consultez la description du champ vads_risk_analysis_result pour plus de détails.</td></tr>
<tr><td>vads_risk_assessment_result</td><td>Liste des actions réalisées sur la transaction, suite au déclenchement des règles de gestion de risque avancée.
Les valeurs possibles sont :
<table>
<tr><th>Valeurs</th><th>Description</th></tr>
<tr><td>ENABLE_3DS</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>DISABLE_3DS</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>NO_PREFERENCE</td><td>• Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.</td></tr>
<tr><td>NO_CHALLENGE_REQUES</td><td>• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).</td></tr>
<tr><td>CHALLENGE_REQUESTED</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge).</td></tr>
<tr><td>CHALLENGE_MANDATE</td><td>• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.</td></tr>
<tr><td>MANUAL_VALIDATION</td><td>• La transaction est créée en validation manuelle.
• La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.</td></tr>
<tr><td>REFUSE</td><td>• La transaction est refusée.</td></tr>
<tr><td>RUN_RISK_ANALYSIS</td><td>• Appel à un analyseur de risques externe sous condition que le marchand possède un contrat.
Se référer à la description du champ vads_risk_analysis_result pour</td></tr>
</table>
</td></tr>
</table>

Tous droits réservés

Nom du champ	Description	
	Valeurs	**Description**
		identifier la liste des valeurs possibles et leur description.
	INFORM	• Une alerte est remontée. • Le marchand est averti qu'un risque est identifié. • Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).

Informations sur le moyen de paiement utilisé :

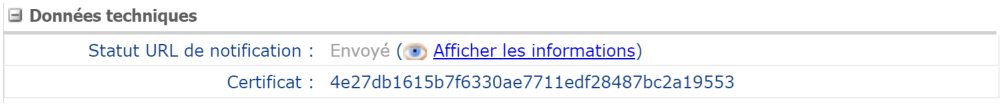
Nom du champ	Remarque
vads_acquirer_network	Code du réseau acquéreur.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice de la carte utilisé.
vads_bank_product	Code produit de la carte utilisée.
vads_card_brand	Moyen de paiement utilisé. Consultez le chapitre **Moyens de paiement compatibles** pour obtenir la liste des valeurs possibles.
vads_card_country	Code pays de la carte utilisée à la norme ISO 3166.
vads_card_number	Numéro de carte tronqué/masqué ou IBAN et BIC utilisés pour le paiement, séparés par un « _ » dans le cas d'un prélèvement ponctuel. Le BIC étant optionnel, il peut ne pas être présent .
vads_expiry_month	Mois d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.
vads_expiry_year	Année d'expiration de la carte utilisée. Il est conseillé d'utiliser cette donnée pour contrôler la date d'expiration de l'alias.

Tous droits réservés

14.7. Test et troubleshooting

Pour tester les notifications, suivez les étapes suivantes :

1. Réalisez un paiement (en mode TEST ou en mode PRODUCTION).
2. Une fois le paiement terminé, recherchez la transaction dans votre Back Office (Menu **Gestion** > **Transactions** ou **Transactions de TEST** si vous avez réalisé le paiement en mode TEST.
3. Double-cliquez sur la transaction pour afficher le **détail de la transaction**.
4. Dans le détail de la transaction, recherchez la section **Données techniques**.
5. Vérifiez le statut de l'URL de notification:



La liste des statuts possibles est donnée ci-dessous:

Statut	Description
N/A	La transaction n'a pas donné lieu a une notification ou aucune règle de notification n'est activée.
URL non définie	Un événement a déclenché la règle de notification de fin de paiement mais l'URL n'est pas configurée.
Appel en cours	La notification est en cours. Ce statut est temporaire.
Envoyé	La notification a bien été envoyée et un équipement distant a répondu avec un code HTTP 200, 201, 202, 203, 204, 205 ou 206.
Envoyé (redirection permanente)	Le site marchand a retourné un code HTTP 301 ou 308 avec une nouvelle URL à contacter. Un nouvel appel en mode POST est réalisé vers la nouvelle URL.
Envoyé (redirection temporaire)	Le site marchand a retourné un code HTTP 302 ou 307 avec une nouvelle URL à contacter. Un nouvel appel en mode POST est réalisé vers la nouvelle URL.
Envoyé (redirection vers une autre page)	Le site marchand a retourné un code HTTP 303 avec une nouvelle URL à contacter. Un nouvel appel en mode GET est réalisé vers la nouvelle URL.
Échoué	Erreur générique différente des codes décrits ci-après.
Serveur injoignable	La notification a duré plus de 35s.
Erreur handshake SSL	La configuration de votre serveur n'est pas correcte. Réalisez un diagnostic sur le site de Qualys (https://www.ssllabs.com/ssltest/) et corrigez les erreurs.
Connexion interrompue	Erreur de communication.
Connexion refusée	Erreur de communication.
Erreur serveur 300	Cas de redirection non supporté par la plateforme.
Erreur serveur 304	Cas de redirection non supporté par la plateforme.
Erreur serveur 305	Cas de redirection non supporté par la plateforme.
Erreur serveur 400	Le site marchand a retourné un code HTTP 400 Bad Request.
Erreur serveur 401	Le site marchand a retourné 'un code HTTP 401 Unauthorized.

Tous droits réservés

Statut	Description
	Assurez-vous que la ressource n'est pas protégée par un fichier .htaccess.
Erreur serveur 402	Le site marchand a retourné un code HTTP 402 Payment Required.
Erreur serveur 403	Le site marchand a retourné un code HTTP 403 Forbidden. Assurez-vous que la ressource n'est pas protégée par un fichier .htaccess.
Erreur serveur 404	Le site marchand a retourné un code HTTP 404 Not Found. Vérifiez que la saisie de l'URL est correcte dans le paramétrage de la règle. Vérifiez aussi que le fichier est bien présent sur votre serveur.
Erreur serveur 405	Le site marchand a retourné un code HTTP 405 Method Not allowed.
Erreur serveur 406	Le site marchand a retourné un code HTTP 406 Not Acceptable.
Erreur serveur 407	Le site marchand a retourné un code HTTP 407 Proxy Authentication Required.
Erreur serveur 408	Le site marchand a retourné un code HTTP 408 Request Time-out.
Erreur serveur 409	Le site marchand a retourné un code HTTP 409 Conflict.
Erreur serveur 410	Le site marchand a retourné un code HTTP 410 Gone.
Erreur serveur 411	Le site marchand a retourné un code HTTP 411 Length Required.
Erreur serveur 412	Le site marchand a retourné un code HTTP 412 Precondition Failed.
Erreur serveur 413	Le site marchand a retourné un code HTTP 413 Request Entity Too Large.
Erreur serveur 414	Le site marchand a retourné un code HTTP 414 Request-URI Too long.
Erreur serveur 415	Le site marchand a retourné un code HTTP 415 Unsupported Media Type.
Erreur serveur 416	Le site marchand a retourné un code HTTP 416 Requested range unsatisfiable.
Erreur serveur 417	Le site marchand a retourné un code HTTP 417 Expectation failed.
Erreur serveur 419	Le site marchand a retourné un code HTTP 419 Authentication Timeout.
Erreur serveur 421	Le site marchand a retourné un code HTTP 421 Misdirected Request.
Erreur serveur 422	Le site marchand a retourné un code HTTP 422 Unprocessable Entity.
Erreur serveur 423	Le site marchand a retourné un code HTTP 423 Locked.
Erreur serveur 424	Le site marchand a retourné un code HTTP 424 Failed Dependency.
Erreur serveur 425	Le site marchand a retourné un code HTTP 425 Too Early.
Erreur serveur 426	Le site marchand a retourné un code HTTP 426 Upgrade Required.
Erreur serveur 429	Le site marchand a retourné un code HTTP 431 Request Header Fields Too Large.
Erreur serveur 431	Le site marchand a retourné un code HTTP 415 Unsupported Media Type.
Erreur serveur 451	Le site marchand a retourné un code HTTP 451 Unavailable For Legal Reasons.
Erreur serveur 500	Le site marchand a retourné un code HTTP 500 Internal Server Error. Une erreur applicative est survenue au niveau du serveur hébergeant votre boutique. Consultez les logs de votre serveur HTTP (le plus souvent apache).

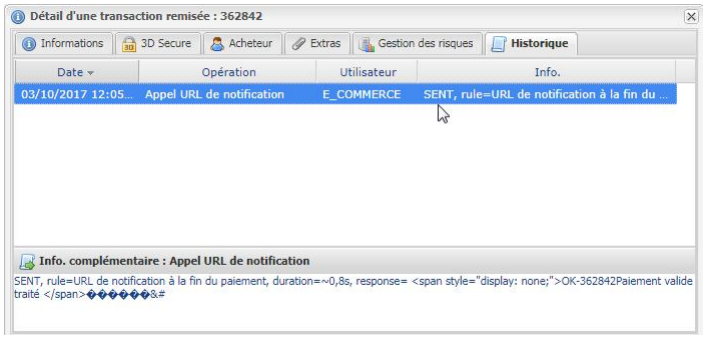
Tous droits réservés

Statut	Description
	Le problème ne peut être corrigé qu'en intervenant sur votre serveur.
Erreur serveur 501	Le site marchand a retourné un code HTTP 501 Not Implemented.
Erreur serveur 502	Le site marchand a retourné un code HTTP 502 Bad Gateway / Proxy Error.
Erreur serveur 503	Le site marchand a retourné un code HTTP 503 Service Unavailable.
Erreur serveur 504	Le site marchand a retourné un code HTTP 504 Gateway Time-out. Le serveur marchand n'a pas accepté l'appel dans le délai imparti de 10s.
Erreur serveur 505	Le site marchand a retourné un code HTTP 505 HTTP Version not supported.

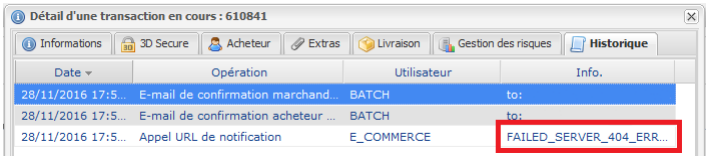
Pour obtenir plus d'informations sur une notification, cliquez sur le lien **Afficher les informations** ou cliquez sur l'onglet **Historique** et recherchez la ligne **Appel URL de notification**.

Afin d'aider le marchand à identifier l'origine de l'erreur, la plateforme analyse systématiquement les 512 premiers caractères retournés par le site marchand et les affiche dans la colonne **Info**.

- Exemple de notification traitée avec succès:



- Exemple de notification en erreur



Si la plateforme n'arrive pas à joindre l'URL de votre page, alors un e-mail d'alerte est envoyé à l'adresse e-mail spécifiée.

Il contient :

- Le code HTTP de l'erreur rencontrée
- Des éléments d'analyse en fonction de l'erreur
- Ses conséquences
- La procédure à suivre depuis le Back Office Expert pour renvoyer la requête vers l'URL définie dans le paramétrage de la règle.

Tous droits réservés

15. OBTENIR DE L'AIDE

Vous cherchez de l'aide ? Consultez notre FAQ.

Pour toute question, contactez le support technique.

Pour faciliter le traitement de vos demandes, préparez votre code client (Exemple : **CLXXXXX**, **MKXXXXX** ou **AGXXXXX**).

Cette information est disponible dans le Back Office Marchand en haut du menu.

Tous droits réservés

16. ANNEXES

16.1. Créer automatiquement un abonnement par Web Services

Utilisez la méthode **Charge/CreateSubscription** pour réaliser des paiements récurrents (abonnements) à partir d'un alias déjà existant et valide.

Pour plus d'informations, consultez la description de la méthode Charge/CreateSubscription.

16.2. Résilier automatiquement un abonnement par Web services

Utilisez la méthode **Subscription/Cancel** pour résilier un abonnement.

Pour plus d'informations, consultez la description de la méthode Subscription/Cancel.

16.3. Cartes de test

Les cartes de test sont disponibles sur la page de paiement.

Elles permettent, en fonction du scénario de test associé à la carte :

- de créer un alias et / ou un paiement récurrent uniquement si le résultat du test est "Paiement accepté".
- de ne pas créer d'alias si le résultat de test est "Paiement refusé".

Pour tester le comportement lorsqu'une échéance est refusée, vous devez utiliser la carte de test suivante :

Numéro de carte	Cas de test vérifié
4970101000001002	Création d'alias OK - Paiement refusé pour cause de plafond dépassé si montant de l'échéance est supérieur à 0.

Remarque

Cette carte n'est pas proposée sur la page de paiement lors de la création d'un alias.

Tous droits réservés