SOLUTION COLLECT

API Formulaire

Guide d'implémentation

Version du document 3.42

Sommaire

1. DÉFINITIONS 5

1.1. Demande d'autorisation 5

1.2. Demande de renseignement 5

1.3. Chaînage des transactions CIT/MIT 5

2. LES DIFFÉRENTS TYPES DE PAIEMENT 7

2.1. Paiement comptant immédiat 7

2.2. Paiement comptant différé 7

2.2.1. Délai de remise inférieur à la durée de validité de l'autorisation 8

2.2.2. Délai de remise supérieur à la durée de validité de l'autorisation 8

2.3. Paiement en plusieurs fois 10

2.4. Paiement complémentaire 16

2.5. Proposer le paiement dans une autre devise 18

2.6. Le service "Autorisations anticipées" 19

2.7. Durée de validité d'une demande d'autorisation 21

3. L'AUTHENTIFICATION 3-D SECURE 26

3.1. Cinématique "Frictionless" 26

3.2. Cinématique "Challenge" 27

3.3. Augmenter les chances de frictionless 28

4. COMPRENDRE LE DÉROULEMENT D'UN PAIEMENT 30

4.1. Définir les étapes d'un paiement - Vue acheteur 30

4.2. Définir les étapes d'un paiement - Vue marchand 33

5. PROPOSER DES TENTATIVES DE PAIEMENT SUPPLÉMENTAIRES 34

6. CYCLE DE VIE DES TRANSACTIONS 35

6.1. Paiement comptant immédiat 35

6.1.1. Validation automatique 35

6.1.2. Validation manuelle 36

6.2. Paiement comptant différé 38

6.2.1. Validation automatique 38

6.2.2. Validation manuelle 39

6.3. Paiement en plusieurs fois 40

6.3.1. Validation automatique 40

6.3.2. Validation manuelle 41

7. ÉTABLIR LE DIALOGUE AVEC LA PLATEFORME DE PAIEMENT 42

7.1. Définir l'URL de la page de paiement 42

7.2. S'identifier lors des échanges 42

7.3. Choisir le mode Test ou Production....44
7.4. Gérer le dialogue vers le site marchand....45
7.5. Gérer la sécurité....47
7.5.1. Garantir l'intégrité des échanges....47
7.5.2. Sélectionner l'algorithme de hachage....48
7.5.3. Conserver la clé de production....48
7.5.4. Gérer les données sensibles....48
7.6. Gérer les paramètres de votre boutique avec un fichier de configuration....49

8. PARAMÉTRER LES NOTIFICATIONS....50
8.1. Notifications des différents statuts pour un paiement comptant immédiat....50
8.2. Notifications des différents statuts pour un paiement comptant différé....51
8.3. Notifications des différents statuts pour les échéances d'un paiement en plusieurs fois....52
8.4. Accéder au centre de notification....53
8.5. Configurer la notification à la fin du paiement....53
8.6. Configurer la notification sur autorisation par batch....55
8.7. Configurer la notification en cas d'abandon ou annulation....56
8.8. Configurer la notification sur une opération provenant du Back Office....57
8.9. Configurer la notification sur modification par batch....58
8.10. Rejeu automatique en cas d'échec....59
8.11. Configurer les e-mails envoyés au marchand....60
8.12. Configurer les e-mails envoyés à l'acheteur....61

9. GÉNÉRER UN FORMULAIRE DE PAIEMENT....63
9.1. Créer un paiement comptant immédiat....65
9.2. Créer un paiement comptant différé....67
9.3. Créer un paiement en plusieurs fois....69
9.4. Créer une autorisation sans remise....72

10. UTILISER DES FONCTIONS COMPLÉMENTAIRES....74
10.1. Gérer le retour vers le site marchand....74
10.2. Activer le retour automatique vers le site marchand....77
10.3. Définir le mode de remise en banque (automatique / manuel)....78
10.4. Transmettre les données de l'acheteur....79
10.5. Transmettre les données de livraison....81
10.6. Transmettre les données de la commande....82
10.7. Transmettre la préférence 3-D Secure....85
10.8. Surcharger l'URL de notification instantanée (IPN)....87
10.9. Définir le contrat commerçant....88
10.10. Créer des champs spécifiques en fonction de vos besoins....91
10.11. Transmettre les données du sous-marchand....92
10.12. Transmettre les données à un ou plusieurs réseaux....92

11. PERSONNALISER LES PAGES DE PAIEMENT....94
11.1. Surcharger le modèle de personnalisation....94

11.2. Gérer les moyens de paiement proposés à l'acheteur 95
11.3. Modifier la langue 96
11.4. Modifier les langues proposées à l'acheteur 97
11.5. Modifier le nom et l'URL de la boutique 98
11.6. Modifier le libellé du bouton « Retourner à la boutique » 99

12. CALCULER LA SIGNATURE 100
12.1. Exemple d'implémentation en JAVA 102
12.2. Exemple d'implémentation en PHP 104

13. ENVOYER LA DEMANDE DE PAIEMENT 105
13.1. Rediriger l'acheteur vers la page de paiement 105
13.2. Gérer les erreurs 105
13.3. Gérer les timeout 107

14. IMPLÉMENTER L'IPN 108
14.1. Préparer son environnement 109
14.2. Récupérer les données retournées dans la réponse 110
14.3. Calculer la signature de l'IPN 111
14.4. Comparer les signatures 112
14.5. Analyser la nature de la notification 113
14.6. Traiter les données de la réponse 114
14.7. Test et troubleshooting 122

15. TRAITER LE RETOUR À LA BOUTIQUE 125

16. OBTENIR DE L'AIDE 126

1. DÉFINITIONS

1.1. Demande d'autorisation

Une demande d'autorisation permet d'accepter ou refuser une transaction.

Elle connecte la banque du porteur (SAE = Système d'Acception Emetteur), la banque du marchand (SAA = Système d'Acceptation Acquéreur), et la plateforme de paiement.

Lorsqu'une demande d'autorisation est acceptée, le plafond de la carte est abaissé du montant autorisé.

1.2. Demande de renseignement

Une demande de renseignement vérifie la validité de la carte sans la débiter.

C'est une demande d'autorisation spécifique avec un montant à 0 EUR.

Si l'acquéreur ne supporte pas cette demande, une demande d'autorisation de 1 EUR est effectué sans remise en banque.

Les porteurs de cartes prépayées ou à débit immédiat voient un débit virtuel de 1 EUR sur leur compte.

Le montant est restauré lorsque l'émetteur annule l'autorisation ce qui peut prendre jusqu'à 30 jours pour les cartes de débit.

Les demandes de renseignement sont envoyées dans les cas suivants :

- Paiement différé, la date de remise en banque est au-delà de la durée de validité de l'autorisation,
- Création ou mise à jour d'un alias de carte sans paiement.

Ces opérations apparaissent dans le Back Office Expert comme une transaction de type "Vérification".

1.3. 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

2. LES DIFFÉRENTS TYPES DE PAIEMENT

2.1. Paiement comptant immédiat

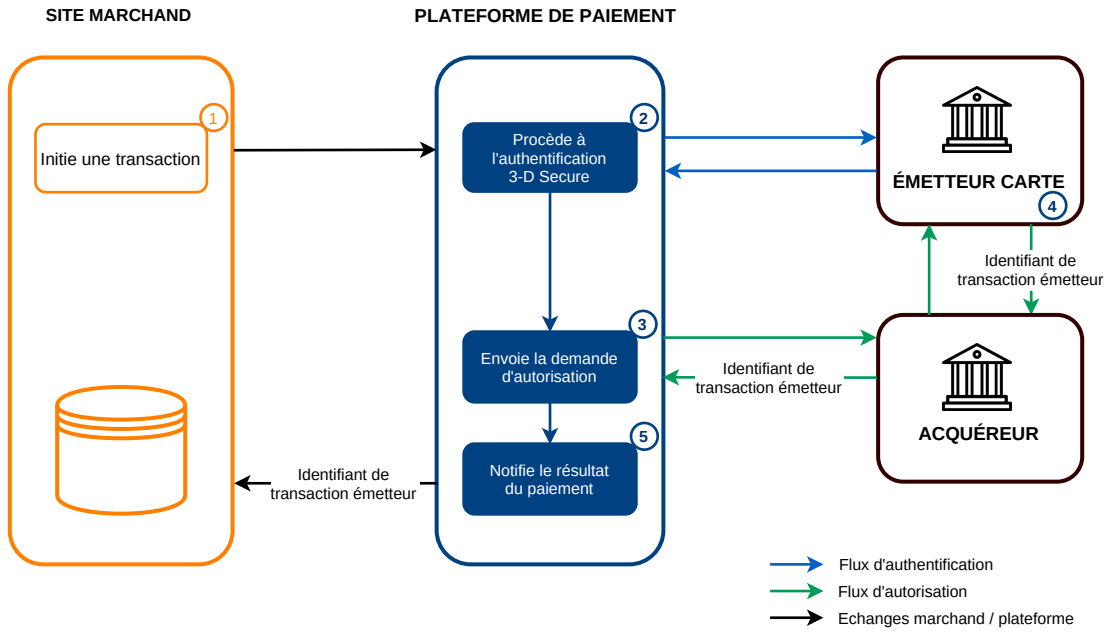
Un paiement est considéré comme comptant immédiat si :

- Le montant est débité en une seule fois,
- Le délai de remise en banque est de 0 jour.

Le paiement est remis en banque dès que possible.

Schéma simplifié

CIT



1. Le site marchand soumet une demande de paiement.
2. La plateforme de paiement initie l'authentification du porteur auprès de l'émetteur (obligatoire pour toutes les transactions CIT).
3. Après l'authentification (challenge ou frictionless), la plateforme demande l'autorisation en fournissant les données d'authentification du porteur.
4. L'émetteur génère et transmet un identifiant unique de transaction dans sa réponse.
5. La plateforme de paiement notifie le site marchand du résultat du paiement.

La plateforme de paiement stocke l'identifiant de transaction émetteur pour chaque transaction.

Si le marchand duplique la transaction (MIT), la plateforme utilise cet identifiant comme référence de chaînage.

La gestion de la référence de chaînage est automatique et transparente pour le marchand.

2.2. Paiement comptant différé

Un paiement est considéré comme comptant différé si :

Tous droits réservés

- Le montant est débité en une seule fois,
- Le délai de remise en banque est strictement supérieur à 0 jour.

  La date de remise ne dépasse pas 12 mois après la date d'enregistrement de la demande de paiement.

La date de remise est calculée comme suit :

Date de remise en banque = date du paiement + délai de remise en banque.

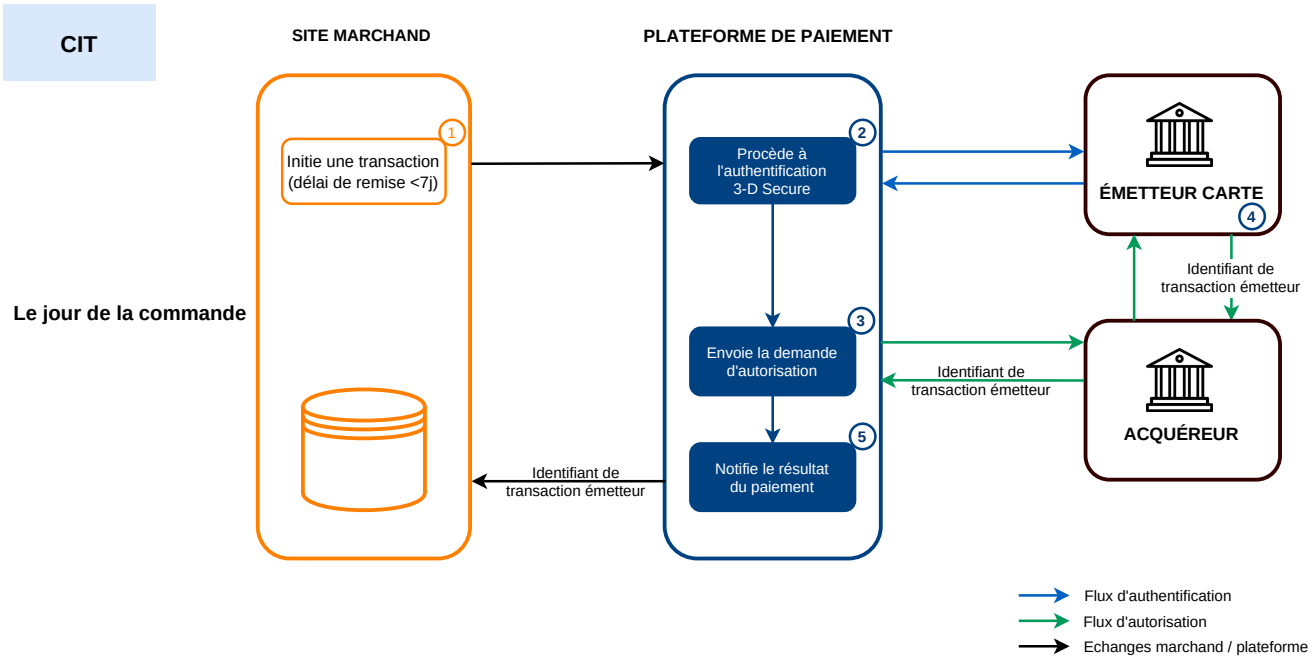
La durée de validité de l' autorisation dépend du moyen de paiement utilisé (voir durée de validité d'une autorisation).

Deux types de paiements comptants différés :

1. **Délai de remise inférieur à la durée de validité de l'autorisation**
2. **Délai de remise supérieur à la durée de validité de l'autorisation**

2.2.1. Délai de remise inférieur à la durée de validité de l'autorisation

Schéma simplifié



Le jour de la commande :

1. Le site marchand soumet une demande de paiement.
2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   La réglementation impose l'authentification du porteur pour toutes les transactions CIT.
3. Après l'authentification (challenge ou frictionless), la plateforme demande l'autorisation en fournissant les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le transmet dans sa réponse.
5. La plateforme de paiement notifie le site marchand du résultat du paiement.

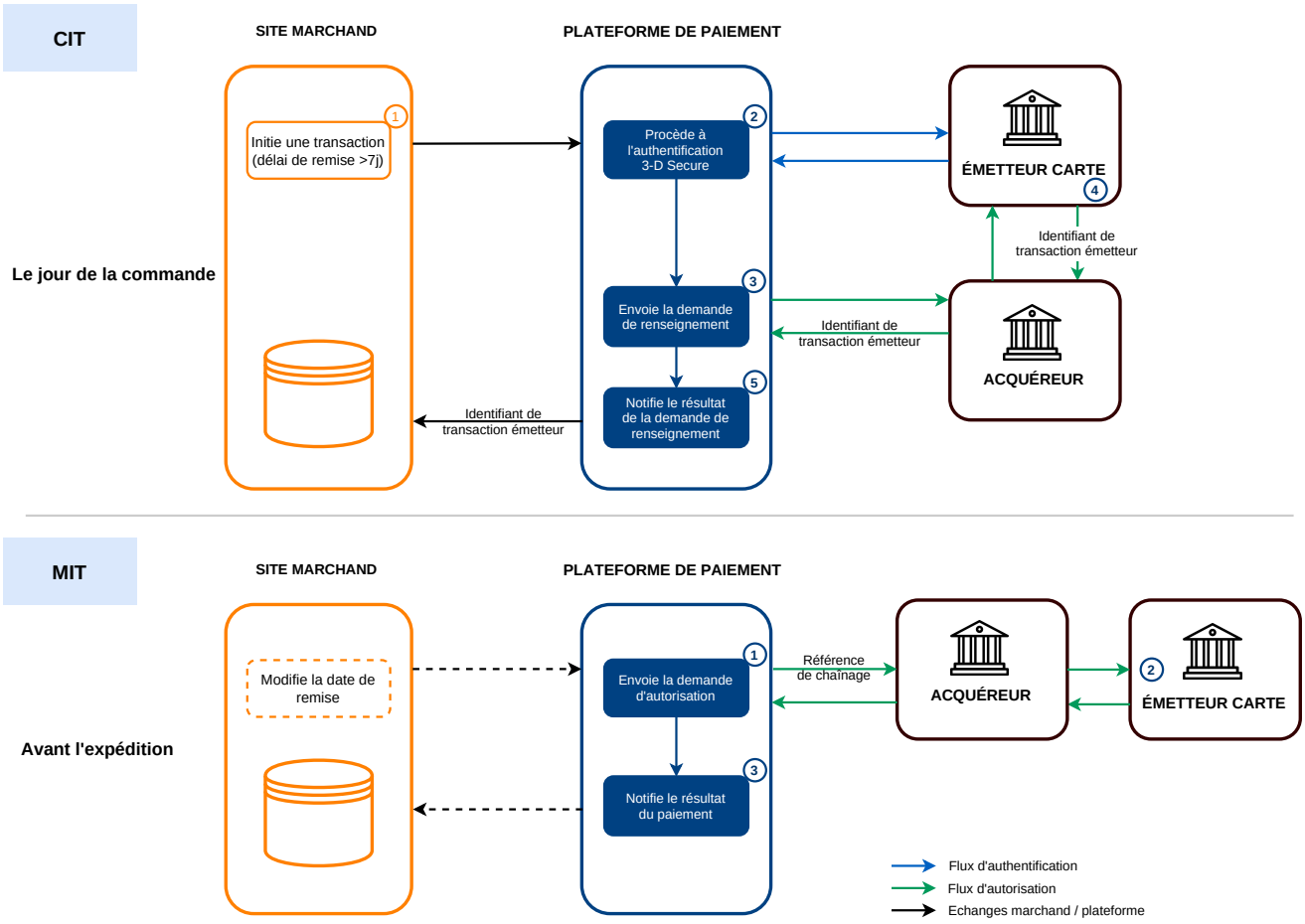
Avant l'expédition :

1. Si l'expédition a lieu avant la date de remise initial, le marchand ajuste la date de remise de remise à J.
2. Si aucune action n'est faite sur la transaction, la transaction est remise en banque à la date demandée initialement.

2.2.2. Délai de remise supérieur à la durée de validité de l'autorisation

Tous droits réservés

Schéma simplifié



Le jour de la commande :

1. Le site marchand soumet une demande de paiement.
2. La plateforme de paiement initie l'authentification du porteur auprès de l'émetteur.

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

Avant l'expédition :

1. Sans action sur la transaction, la demande d'autorisation est réalisée à J-1 avant la date de remise demandée.

   Si l'expédition a lieu avant la date de remise initial, le marchand ajuste la date de remise de remise à J.

   La plateforme de paiement réalise une demande d'autorisation et fournit l'identifiant de transaction initiale (CIT) comme référence de chaînage.
2. L'émetteur identifie la transaction comme une MIT liée à une série de paiements où le porteur s'est authentifié préalablement.

   La transaction n'est pas refusée pour défaut d'authentification (soft decline).
3. Si le marchand a activé la règle de notification "URL de notification sur autorisation par batch", la plateforme de paiement notifie le site marchand du résultat du paiement.

Tous droits réservés

2.3. Paiement en plusieurs fois

Un paiement est dit "en plusieurs fois" lorsque l'acheteur est débité en plusieurs échéances.

La première échéance fonctionne comme un paiement comptant immédiat, les échéances suivantes sont similaires à des paiements comptants différés.

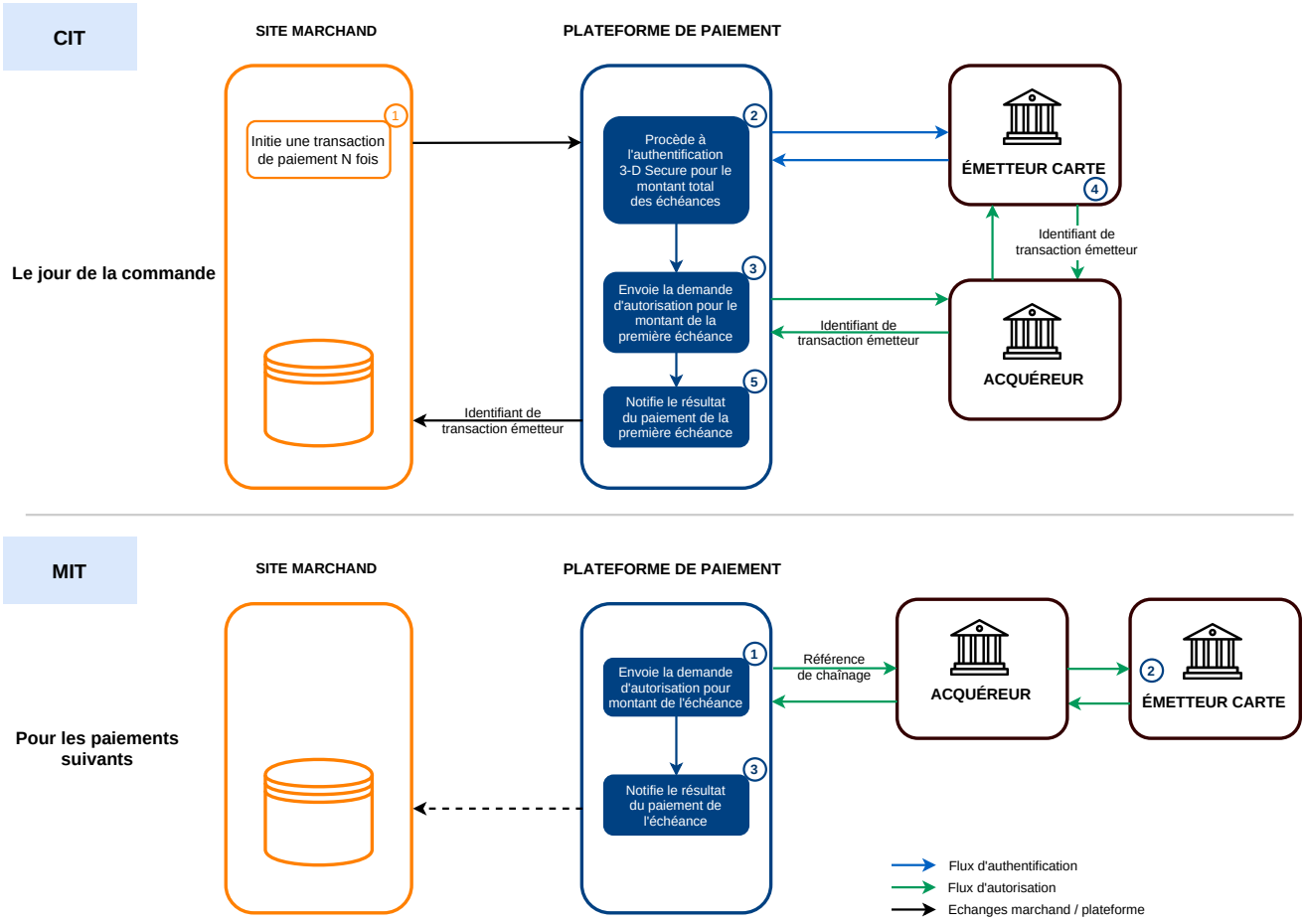
Seule la première échéance peut être garantie pour le marchand, à condition que la date de présentation de cette échéance soit inférieure à la date de validité de l'autorisation, selon le moyen de paiement (voir : Durée de validité d'une demande d'autorisation à la page 21) .

Dans le cadre de l'application de la DSP2, le porteur devra se soumettre à une authentification forte lors du paiement de la première échéance.

Si la demande d'autorisation (ou de renseignement) est acceptée le jour de la commande, une transaction est créée pour chaque échéance du paiement en plusieurs fois.

Dans le cas contraire, une seule transaction refusée est créée. L'onglet **Historique** dans le Back Office Expert indique le nombre d'échéances initialement prévues.

Schéma simplifié



Le jour de la commande :

1. Le site marchand soumet une demande de paiement en plusieurs fois.
2. La plateforme de paiement initie le processus d'authentification du porteur auprès de l'émetteur.

   L'authentification est requise pour le montant total des échéances. La réglementation impose une authentification forte.

Tous droits réservés

3. Après l'authentification forte, la plateforme fait une demande d'autorisation sur le montant de la première échéance et fournit les données d'authentification du porteur.
4. L'émetteur génère un identifiant unique de transaction et le renvoie dans sa réponse.
5. La plateforme de paiement notifie le site marchand du résultat du paiement.

Pour les paiements suivants :

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 précédemment authentifiés par le porteur et procède à la demande d'autorisation.

   La transaction n'est pas refusée pour défaut d'authentification (soft decline).
3. Si le marchand a activé l'URL de notification sur autorisation par batch, 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.

Un contrôle est effectué pour vérifier la validité du moyen de paiement sur toute la durée de l'échéancier.

En cas d'invalidité de carte, un message d'avertissement est affiché à l'acheteur, qui doit utiliser un autre moyen de paiement ou abandonner le paiement.

Cependant, si la carte est renouvelée ou résiliée avant la fin de l'échéancier, les paiements seront refusés par la banque émettrice (code retour auto 54: Date de validité du moyen de paiement dépassée).

Dans ce cas, vous recevez un e-mail d'avertissement via la règle de notification "E-mail de refus échéance de paiement en N fois".

Liste des moyens de paiement compatibles avec le paiement en plusieurs fois :

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement en plusieurs fois
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	✗

Tous droits réservés

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement en plusieurs fois
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 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	✗
AMEXGLOBAL	American Express	AMEX	✓
APPLE PAY	Paiement par Wallet Apple Pay	APPLE_PAY	✗
AURORE	Carte Cpay	AURORE-MULTI	✗
BIZUM	Bizum	BIZUM	✗
CB	CB	CB	✓
CB	Carte virtuelle e-Carte Bleue	E-CARTEBLEUE	✓
CB	Maestro	MAESTRO	✓
CB	Mastercard	MASTERCARD	✓
CB	Visa	VISA	✓
CB	Visa Electron	VISA_ELECTRON	✓
CB	VPay	VPAY	✓
CB	Carte Titre-Restaurant Apetiz	APETIZ	✓
CB	Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	✓
CB	Titre-Restaurant Mastercard 1ère génération	EDENRED	✓
CB	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	✗

Tous droits réservés

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement en plusieurs fois
COFIDIS	Cofidis en 10 ou 60 fois (France)	COFIDIS_LOAN_FR	✗
COFIDIS	Cofidis Pay Later (France)	COFIDIS_DFPAY_FR	✗
COFIDIS	Cofidis en 4 fois (Espagne)	COFIDIS_4X_ES	✗
COFIDIS	Cofidis en 5 ou 12 fois (Espagne)	COFIDIS_LOAN_ES	✗
CONECS	Carte Titre-Restaurant Bimpli (ex Apetiz)	APETIZ	✗
CONECS	Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	✗
CONECS	Carte Titre-Restaurant Conecs	CONECS	✗
CONECS	Carte Titre-Restaurant Sodexo	SODEXO	✗
CVCONNECT	Chèque-Vacances Connect	CVCO	✗
DFS	Diners	DINERS	✗
DFS	Discover	DISCOVER	✗
EDENRED	Ticket EcoChèque Edenred	EDENRED_EC	✗
EDENRED	Ticket Compliments Edenred	EDENRED_TC	✗
EDENRED	Ticket Restaurant Edenred	EDENRED_TR	✗
EDENRED	Ticket Sport & Culture Edenred	EDENRED_SC	✗
EDENRED	Ticket Chèque Consommation	EDENRED_CC	✗
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 3X Franfinance	FRANFINANCE_3X	✗
FRANFINANCE	Paiement en 4X Franfinance	FRANFINANCE_4X	✗
FRANFINANCE_SB	Paiement en 3X Franfinance - Mode sandbox	FRANFINANCE_3X	✗

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement en plusieurs fois
FRANFINANCE_SB	Paiement en 4X 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	✓
GATECONEX	Visa Electron	VISA_ELECTRON	✗
GATECONEX	VPay	VPAY	✗
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 Electron	VISA_ELECTRON	✗
GICC_VISA	VPay	VPAY	✗
GOOGLEPAY	Paiement par Wallet Google Pay	GOOGLEPAY	✗
ILLICADO	Cartes Cadeau Illicado	ILLICADO	✗
JCB	JCB	JCB	✓
LYRA_COLLECT_PPRO	Alipay	ALIPAY	✗
LYRA_COLLECT_PPRO	Bancontact Mistercash	BANCONTACT	✗
LYRA_COLLECT_PPRO	iDeal Internet Banking	IDEAL	✗
LYRA_COLLECT_PPRO	Multibanco	MULTIBANCO	✗

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement en plusieurs fois
LYRA_COLLECT_PPRO	MyBank	MYBANK	✗
LYRA_COLLECT_PPRO	Przelewy24	PRZELEWY24	✗
LYRA_COLLECT_PPRO	UnionPay	UNION_PAY	✗
LYRA_COLLECT_PPRO	WeChat	WECHAT	✗
MULTIBANCO	MB Reference	MULTIBANCO	✗
MULTIBANCO	MB Way	MB_WAY	✗
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_SANDBOX	FacilyPay Oney - Mode sandbox	ONEY_SANDBOX	✗
ONEY	FacilyPay Oney	ONEY	✗
PAYDIREKT_V2	PayDirekt	PAYDIREKT	✗
PAYCONIQ	Payconiq	PAYCONIQ	✗
PAYPAL	PayPal	PAYPAL	✗
PAYPAL_SB	PayPal - Mode sandbox	PAYPAL_SB	✗
PAYPAL_BNPL	PayPal Pay Later	PAYPAL_BNPL	✗
PAYPAL_BNPL_SB	PayPal Pay Later - Mode sandbox	PAYPAL_BNPL_SB	✗
PLANET_DCC	MASTERCARD	MASTERCARD	✓
PLANET_DCC	VISA	VISA	✓
POSTFINANCEV2	PostFinance	POSTFINANCE	✗
POSTFINANCEV2	PostFinance E-finance	POSTFINANCE_EFIN	✗

Tous droits réservés

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Supporte le paiement en plusieurs fois
REDSYS_REST	American Express	AMEX	✅
REDSYS_REST	Diners Club	DINERS	✅
REDSYS_REST	JCB	JCB	✅
REDSYS_REST	Maestro	MAESTRO	❌
REDSYS_REST	Mastercard	MASTERCARD	✅
REDSYS_REST	Visa	VISA	✅
REDSYS_REST	Visa Electron	VISA_ELECTRON	❌
SAMSUNG PAY	Paiement par Wallet Samsung Pay	SAMSUNG_PAY	❌
SEPA	Prélèvement Bancaire SEPA DIRECT DEBIT	SDD	❌
WECHAT_PAY	WeChat Pay	WECHAT	❌

2.4. Paiement complémentaire

Le paiement complémentaire permet à l'acheteur de régler une commande en utilisant plusieurs moyens de paiement.

Il existe deux cas d'utilisation :

1. L'acheteur règle la totalité du paiement avec sa carte cadeau ou privative.
2. L'acheteur utilise plusieurs moyens de paiement pour régler la commande.

   Par exemple, il peut payer une partie avec une carte cadeau ou privative et le complément avec une carte bancaire.

Liste des moyens de paiement compatibles :

- Cartes enseignes

Moyen de paiement	Code technique
Carte enseigne Accord	ACCORD_STORE
Carte enseigne Alinéa	ALINEA
Carte enseigne Auchan	AUCHAN
Carte enseigne Boulanger	BOULANGER
Carte enseigne Leroy-Merlin	LEROY-MERLIN
Carte enseigne Norauto	NORAUTO
Carte enseigne PicWic	PICWIC
Carte enseigne Villaverde	VILLAVERDE
Carte enseigne Accord - Mode sandbox	ACCORD_STORE_SB
Carte enseigne Auchan - Mode sandbox	AUCHAN_SB

Moyen de paiement	Code technique
Carte enseigne Boulanger - Mode sandbox	BOULANGER_SB
Carte enseigne Leroy-Merlin - Mode sandbox	LEROY-MERLIN_SB
Carte enseigne Norauto - Mode sandbox	NORAUTO_SB
Carte enseigne PicWic - Mode sandbox	PICWIC_SB
Carte enseigne Villaverde - Mode sandbox	VILLAVERDE_SB

- Cartes cadeaux

Moyen de paiement	Code technique
Carte cadeau Alinéa	ALINEA_CDX
Carte cadeau AlloBébé	ALLOBEBE_CDX
Carte cadeau BizzBee	BIZZBEE_CDX
Carte cadeau Brice	BRICE_CDX
Cartes Cadeau Illicado	ILLICADO
Carte cadeau JouéClub	JOUECLUB_CDX
Carte cadeau AlloBébé - Mode sandbox	ALLOBEBE_CDX_SB
Carte cadeau BizzBee - Mode sandbox	BIZZBEE_CDX_SB
Carte cadeau Brice - Mode sandbox	BRICE_CDX_SB
Carte cadeau Illicado - Mode sandbox	ILLICADO_SB
Carte cadeau JouéClub - Mode sandbox	JOUECLUB_CDX_SB

- Cartes Titre-Restaurant

Moyen de paiement	Code technique
Carte Titre-Restaurant Bimpli (ex Apetiz)	APETIZ
Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ
Carte Titre-Restaurant Conecs	CONECS
Carte Titre-Restaurant Sodexo	SODEXO
Carte Titre-Restaurant EDENRED	EDENRED

- Carte Tickets électroniques - Edenred Belgique

Moyen de paiement	Code technique
Ticket Restaurant	EDENRED_TR
Ticket EcoCheque	EDENRED_EC
Ticket Compliments	EDENRED_TC
Ticket Sport & Culture	EDENRED_SC

- Chèque-Vacances Connect

Moyen de paiement	Code technique
Chèque-Vacances Connect	CVCO

2.5. Proposer le paiement dans une autre devise

Le paiement en devises avec conversion permet aux marchands de proposer des catalogues de prix dans différentes devises sans avoir à gérer de comptabilité dans des devises autres que celle de leur contrat.

Lorsque la plateforme reçoit le montant dans une devise non gérée par vos contrats, elle fait une conversion vers la devise de la société, basée sur le taux de change, fourni quotidiennement par Visa.

L'acheteur est informé du cours indicatif au moment du paiement, mais ne sait pas réellement le montant final de la transaction.

La remise en banque ne se fait pas forcément le jour de l'autorisation, le cours peut varier entre la date d'autorisation et la date de remise.

Ainsi, la contre-valeur affichée lors du paiement est donnée à titre indicatif.

- La demande d'autorisation est envoyée en devise du contrat à l'émetteur de la carte.
- La capture est faite exclusivement dans la devise du contrat.
- L'acheteur est débité dans la devise du contrat, avec des frais de change appliqués par sa banque, sans contrôler le taux de change.

A la fin du paiement, le marchand reçoit une notification contenant les champs suivant :

- **vads_amount** : le montant en devise,
- **vads_currency**: la devise,
- **vads_effective_amount** : le montant réel dans la devise du contrat, calculé en fonction du taux de change en vigueur au moment de l'autorisation,
- **vads_effective_currency** : la devise dans laquelle est faite la capture,
- **vads_change_rate** : le taux de change appliqué pour convertir le montant en devise du contrat vers la devise de l'acheteur.

Tous droits réservés

2.6. Le service "Autorisations anticipées"

Ce service permet de réaliser une demande d'autorisation plusieurs jours avant la date de remise souhaitée.

Le délai dépend de la durée de validité de autorisation et du moyen de paiement utilisé (voir durée de validité d'une autorisation).

En cas de refus de l'émetteur pour un motif non frauduleux, un processus automatique réitère les demandes d'autorisation jusqu'à 2 jours avant la date de remise en banque.

Le marchand peut annuler la transaction ou modifier le montant (à la baisse uniquement) et/ou la date de remise à tout moment.

Ce processus s'applique aux :

- Paiements récurrents
- Paiements différés
- Échéances autres que la première, pour un paiement en plusieurs fois.

En cas de refus pour un motif frauduleux la transaction est définitivement refusée.

Ci dessous la liste des motifs frauduleux qui ne permettent pas le rejeu de l'autorisation.

Réseau	Codes retour autorisation	Libellé
CB	03	Accepteur invalide
	04	Conserver la carte
	05	Ne pas honorer
	07	Conserver la carte, conditions spéciales
	12	Transaction invalide
	13	Montant invalide
	14	Numéro de porteur invalide
	15	Emetteur de carte inconnu
	31	Identifiant de l'organisme acquéreur inconnu
	33	Date de validité de la carte dépassée
	34	Suspicion de fraude
	41	Carte perdue
	43	Carte volée
	54	Date de validité de la carte dépassée
	56	Carte absente du fichier
	57	Transaction non permise à ce porteur
	59	Transaction non permise à ce porteur
	63	Règles de sécurité non respectée
	76	Porteur déjà en opposition, ancien enregistrement conservé
	80	Le paiement sans contact n'est pas admis par l'émetteur

Tous droits réservés

Réseau	Codes retour autorisation	Libellé
	81	Le paiement non sécurisé n'est pas admis par l'émetteur
	82	Révocation paiement récurrent pour la carte chez le commerçant ou pour le MCC et la carte
	83	Révocation tous paiements récurrents pour la carte

Contactez l'administration des ventes si vous souhaitez activer les autorisations anticipées.

2.7. Durée de validité d'une demande d'autorisation

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Durée de validité d'une autorisation (en jours)
ALIPAY_PLUS	Akulaku PayLater ID	AKULAKU_ID	0
ALIPAY_PLUS	Akulaku PayLater PH	AKULAKU_PH	0
ALIPAY_PLUS	Alipay CN (Chine)	ALIPAY_CN	0
ALIPAY_PLUS	Alipay HK (Hong Kong)	ALIPAY_HK	0
ALIPAY_PLUS	BillEase	BILLEASE	0
ALIPAY_PLUS	Boost	BOOST	0
ALIPAY_PLUS	BPI	BPI	0
ALIPAY_PLUS	Dana	DANA	0
ALIPAY_PLUS	GCash	GCASH	0
ALIPAY_PLUS	Kakao Pay	KAKAOPAY	0
ALIPAY_PLUS	Krevido	KREDIVO_ID	0
ALIPAY_PLUS	Maya	MAYA	0
ALIPAY_PLUS	MPay	MPAY	0
ALIPAY_PLUS	Rabbit LINE Pay	RABBIT_LINE_PAY	0
ALIPAY_PLUS	Touch 'n Go eWallet	TNG	0
ALIPAY_PLUS	Toss Pay	TOSS	0
ALIPAY_PLUS	TrueMoney Wallet	TRUEMONEY	0
ALMA	Alma en 2 fois	ALMA_2X	0
ALMA	Alma en 3 fois	ALMA_3X	0
ALMA	Alma en 4 fois	ALMA_4X	0
ALMA	Alma en 10 fois	ALMA_10X	0
ALMA	Alma en 12 fois	ALMA_12X	0
AMEXGLOBAL	American Express	AMEX	7
APPLE PAY	Paiement par Wallet Apple Pay	APPLE_PAY	Selon la carte de paiement
AURORE	Carte Cpay	AURORE-MULTI	29
BIZUM	Bizum	BIZUM	0
CB	CB	CB	7
CB	Carte virtuelle e-Carte Bleue	E-CARTEBLEUE	7
CB	Maestro	MAESTRO	30
CB	Mastercard	MASTERCARD	7

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Durée de validité d'une autorisation (en jours)
CB	Visa	VISA	7
CB	Visa Electron	VISA_ELECTRON	7
CB	VPay	VPAY	7
CB	Carte Titre-Restaurant Bimpli (ex Apetiz)	APETIZ	7
CB	Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	7
CB	Titre-Restaurant Mastercard 1ère génération	EDENRED	7
CB	Carte Titre-Restaurant Sodexo	SODEXO	7
COFIDIS	Cofidis en 3 fois (France)	COFIDIS_3X_FR	6
COFIDIS	Cofidis en 4 fois (France)	COFIDIS_4X_FR	6
COFIDIS	Cofidis en 5 ou 12 fois (France)	COFIDIS_LOAN_CB	6
COFIDIS	Cofidis Pay (France)	COFIDIS_PAY_FR	6
COFIDIS	Cofidis en 10 ou 60 fois (France)	COFIDIS_LOAN_FR	6
COFIDIS	Cofidis Pay Later (France)	COFIDIS_DFPAY_FR	15/30/45
COFIDIS	Cofidis en 4 fois (Espagne)	COFIDIS_4X_ES	6
COFIDIS	Cofidis en 5 ou 12 fois (Espagne)	COFIDIS_LOAN_ES	6
CONECS	Carte Titre-Restaurant Bimpli (ex Apetiz)	APETIZ	30
CONECS	Carte Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	30
CONECS	Carte Titre-Restaurant Conecs	CONECS	30
CONECS	Carte Titre-Restaurant Sodexo	SODEXO	30
CVCONNECT	Chèque-Vacances Connect	CVCO	6
DFS	Diners Club	DINERS	7
DFS	Discover	DISCOVER	7
EDENRED	Ticket EcoChèque Edenred	EDENRED_EC	0
EDENRED	Ticket Chèque Consommation	EDENRED_CC	0
EDENRED	Ticket Compliments Edenred	EDENRED_TC	0
EDENRED	Ticket Restaurant Edenred	EDENRED_TR	0

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Durée de validité d'une autorisation (en jours)
EDENRED	Ticket Sport & Culture Edenred	EDENRED_SC	0
FLOA	Floa en 3 fois	FLOA_3X	7
FLOA	Floa en 4 fois	FLOA_4X	7
FLOA	Floa en 10 fois	FLOA_10X	7
FLOA	Floa Pay Later	FLOA_PAYLATER	30
FRANFINANCE	Paiement en 3X Franfinance	FRANFINANCE_3X	0
FRANFINANCE	Paiement en 4X Franfinance	FRANFINANCE_4X	0
FRANFINANCE_SB	Paiement en 3X Franfinance - Mode sandbox	FRANFINANCE_3X	0
FRANFINANCE_SB	Paiement en 4X Franfinance - Mode sandbox	FRANFINANCE_4X	0
FULLCB	Paiement en 3x sans frais par BNPP PF	FULLCB3X	7
FULLCB	Paiement en 4x sans frais par BNPP PF	FULLCB4X	7
GATECONEX	Bancontact	BANCONTACT	30
GATECONEX	Diners Club	DINERS	3
GATECONEX	Discover	DISCOVER	5
GATECONEX	Carte virtuelle e-Carte Bleue	E-CARTEBLEUE	7
GATECONEX	Maestro	MAESTRO	30
GATECONEX	Mastercard	MASTERCARD	7
GATECONEX	Visa	VISA	7
GATECONEX	Visa Electron	VISA_ELECTRON	7
GATECONEX	VPay	VPAY	7
GICC_DINERS	Diners Club	DINERS	3
GICC_DINERS	Discover	DISCOVER	5
GICC_MAESTRO	Bancontact	BANCONTACT	30
GICC_MAESTRO	Maestro	MAESTRO	30
GICC_MASTERCARD	Mastercard	MASTERCARD	7
GICC_VISA	Visa	VISA	7
GICC_VISA	Visa Electron	VISA_ELECTRON	7
GICC_VISA	VPay	VPAY	7

Tous droits réservés

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Durée de validité d'une autorisation (en jours)
GOOGLEPAY	Paiement par Wallet Google Pay	GOOGLEPAY	Selon la carte de paiement
ILLICADO	Cartes Cadeau Illicado	ILLICADO	0
IP	Virement bancaire	IP_WIRE	90
IP	Virement bancaire instantané	IP_WIRE_INST	0
JCB	JCB	JCB	7
LYRA_COLLECT_PPRO	Alipay	ALIPAY	0
LYRA_COLLECT_PPRO	Bancontact	BANCONTACT	0
LYRA_COLLECT_PPRO	iDeal Internet Banking	IDEAL	0
LYRA_COLLECT_PPRO	Multibanco	MULTIBANCO	0
LYRA_COLLECT_PPRO	MyBank	MYBANK	0
LYRA_COLLECT_PPRO	Przelewy24	PRZELEWY24	0
LYRA_COLLECT_PPRO	UnionPay	UNION_PAY	0
LYRA_COLLECT_PPRO	WeChat	WECHAT	0
MULTIBANCO	MB Reference	MULTIBANCO	0
MULTIBANCO	MB Way	MB_WAY	0
ONEY_API	Paiement 3x 4x Oney	ONEY_3X_4X	0
ONEY_API	Paiement 10x 12x Oney	ONEY_10X_12X	0
ONEY_API	Paiement Oney Pay Later	ONEY_PAYLATER	0
ONEY_API	Cartes Enseignes partenaires d'Oney.	ONEY_ENSEIGNE	0
ONEY_API_SANDBOX	Paiement 3x 4x Oney en mode sandbox	ONEY_3X_4X	0
ONEY_API_SANDBOX	Paiement 10x 12x Oney en mode sandbox	ONEY_10X_12X	0
ONEY_API_SANDBOX	Paiement Oney Pay Later en mode sandbox	ONEY_PAYLATER	0
ONEY_API_SANDBOX	Cartes Enseignes partenaires d'Oney en mode sandbox.	ONEY_ENSEIGNE	0
ONEY_SANDBOX	FacilyPay Oney - Mode sandbox	ONEY_SANDBOX	255
ONEY	FacilyPay Oney	ONEY	255
PAYDIREKT_V2	PayDirekt	PAYDIREKT	7
PAYCONIQ	Payconiq	PAYCONIQ	0
PAYPAL	PayPal	PAYPAL	3

Tous droits réservés

Code Réseau	Moyen de paiement	Type de cartes (vads_payment_cards)	Durée de validité d'une autorisation (en jours)
PAYPAL	PayPal Pay Later	PAYPAL_BNPL	3
PAYPAL_SB	PayPal - Mode sandbox	PAYPAL_SB	3
PAYPAL_SB	PayPal Pay Later - Mode sandbox	PAYPAL_BNPL_SB	3
PLANET_DCC	MASTERCARD	MASTERCARD	0
PLANET_DCC	VISA	VISA	0
POSTFINANCEV2	PostFinance	POSTFINANCE	1
POSTFINANCEV2	PostFinance E-finance	POSTFINANCE_EFIN	1
REDSYS_REST	American Express	AMEX	28
REDSYS_REST	Diners Club	DINERS	28
REDSYS_REST	JCB	JCB	28
REDSYS_REST	Maestro	MAESTRO	28
REDSYS_REST	Mastercard	MASTERCARD	28
REDSYS_REST	Visa	VISA	28
REDSYS_REST	Visa Electron	VISA_ELECTRON	28
SAMSUNG PAY	Paiement par Wallet Samsung Pay	SAMSUNG_PAY	Selon la carte de paiement
SEPA	Prélèvement Bancaire SEPA DIRECT DEBIT	SDD	15
NPCIUPI	BHIM UPI	UPI	0
WECHAT_PAY	WeChat Pay	WECHAT	0

Tous droits réservés

3. L'AUTHENTIFICATION 3-D SECURE

Retrouvez toutes les informations utiles sur l'authentification 3DS dans le guide du 3-D Secure.

3.1. Cinématique "Frictionless"

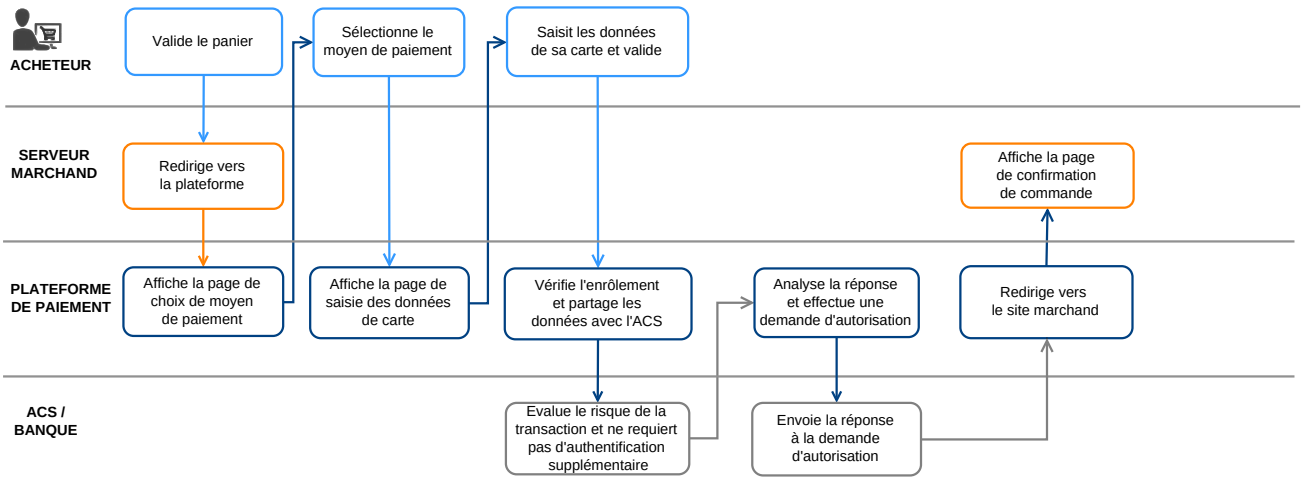
Dans une cinématique frictionless (sans interaction de l'acheteur), l'émetteur peut déterminer, à partir des informations reçues :

- Aucune authentification supplémentaire n'est requise.

  La plateforme de paiement poursuit le paiement et procède à la demande d'autorisation.

- Les informations analysées ne permettent pas de continuer le paiement.

  La plateforme de paiement notifie le site marchand du refus et redirige l'acheteur vers le site marchand en l'informant du refus.



Tous droits réservés

3.2. Cinématique "Challenge"

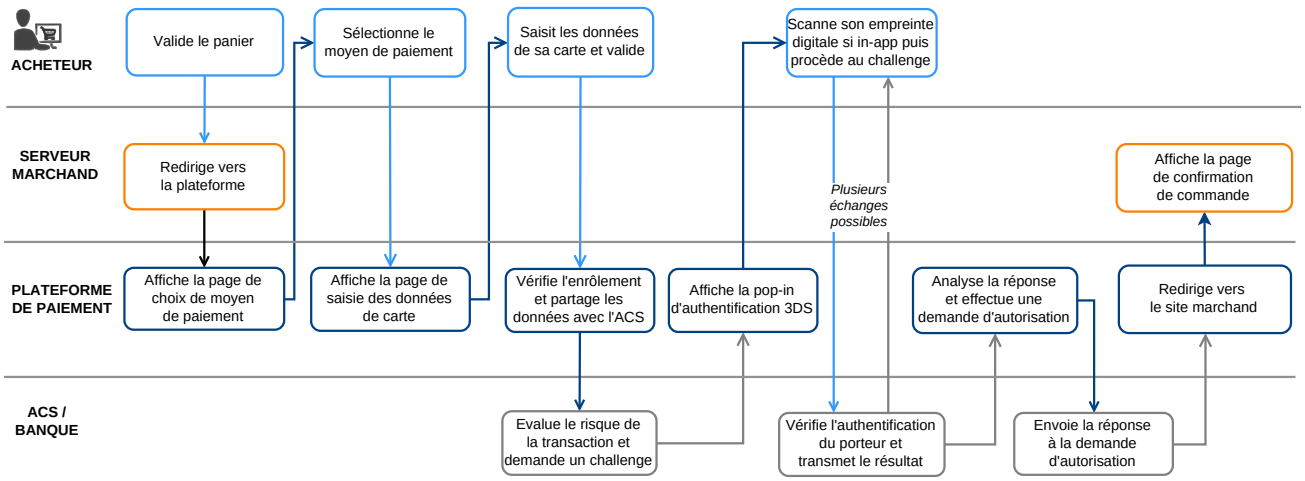
Dans une cinématique de challenge, l'émetteur détermine, à partir des informations reçues, qu'une interaction avec l'acheteur est nécessaire, à travers :

- Un élément biométrique comme l'empreinte digitale,
- Une authentification forte à deux facteurs.

Pour les solutions in-app, l'empreinte digitale est systématiquement demandée avant de procéder au challenge.

Une fois le challenge terminé avec succès, la plateforme de paiement poursuit le paiement et procède à la demande d'autorisation.

En cas d'erreur technique ou de mauvaise authentification, le paiement s'arrête. La plateforme de paiement notifie le marchand du refus et redirige l'acheteur vers le site marchand en l'informant du refus



Tous droits réservés

3.3. Augmenter les chances de frictionless

L'utilisation de ces champs est optionnelle. C'est toujours la banque émettrice qui décide si une authentification forte est réalisée ou non.

Nom / Description	Format / Valeurs
vads_cust_address_number Numéro de rue - Adresse de facturation.	Format : ans..64
vads_cust_address2 2ème ligne d'adresse - Adresse de facturation.	Format : ans..255
vads_cust_address 1ère ligne d'adresse - Adresse de facturation.	Format : ans..255
vads_cust_cell_phone Numéro de téléphone mobile.	Format : an..32
vads_cust_city Ville - Adresse de facturation.	Format : an..128
vads_cust_email Adresse e-mail du porteur de carte.	Format : ans..150
vads_cust_national_id Identifiant national. Permet d'identifier de façon unique chaque citoyen au sein d'un pays.	Format : ans..255
vads_cust_phone Numéro de téléphone.	Format : an..32
vads_cust_state Etat / Région - Adresse de facturation.	Format : ans..127
vads_cust_zip Code postal- Adresse de facturation.	Format : an..64
vads_ship_to_city Ville - Adresse de livraison.	Format : an..128
vads_ship_to_email Adresse e-mail de livraison dans le cas d'une commande e-ticket.	Format : an..128
vads_ship_to_type Type de transport	Format : enum Valeurs pour 3DS2 : • **RECLAIM_IN_SHOP** : Retrait de la marchandise en magasin. • **RELAY_POINT** : Réseau de points de retrait tiers (Kiala, Alveol, etc). • **RECLAIM_IN_STATION** : Retrait dans un aéroport, une garre ou une agence de voyage. • **PACKAGE_DELIVERY_COMPANY** : Livraison par transporteur (Colissimo, UPS, etc).

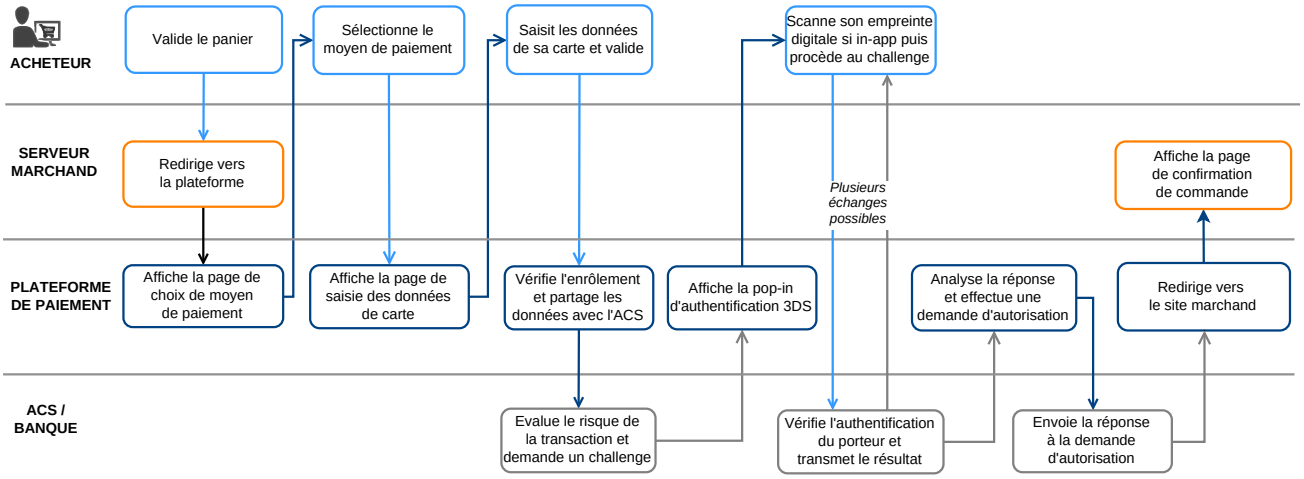
Nom / Description	Format / Valeurs
	• **ETICKET** : Emission d'un billet électronique, téléchargement. • **CARD_HOLDER_ADDRESS** : Livraison chez l'acheteur. • **VERIFIED_ADDRESS** : Livraison à une adresse vérifiée (Adresse de livraison et de facturation identiques). • **NOT_VERIFIED_ADDRESS** : Livraison à une adresse non vérifiée (Adresse de livraison et de facturation différentes). • **SHIP_TO_STORE** : Livraison en magasin. • **DIGITAL_GOOD** : Livraison digitale. • **ETRAVEL_OR_ETICKET** : Billet électronique. • **OTHER** : Autre. • **PICKUP_POINT** : Retrait en point relais. • **AUTOMATED_PICKUP_POINT** Retrait en point relais automatique.
vads_ship_to_state Etat / Région - Adresse de livraison.	Format : ans..127
vads_ship_to_street2 2ème ligne d'adresse - Adresse de livraison.	Format : ans..255
vads_ship_to_street 1ère ligne d'adresse - Adresse de livraison.	Format : ans..255
vads_ship_to_speed Rapidité de livraison	Format : enum Valeurs pour 3DS2 : • **STANDARD** : Livraison standard. • **EXPRESS** : Livraison en moins de 24 h. • **PRIORITY**: Livraison prioritaire. • **ELECTRONIC_DELIVERY** : Téléchargement électronique. • **SAME_DAY_SHIPPING** : Livraison le même jour. • **OVERNIGHT_SHIPPING** : Livraison de nuit. • **TWO_DAYS_OR_MORE_SHIPPING** : Livraison 2 jours ou plus.
vads_ship_to_zip Code postal - Adresse de livraison.	Format : ans..64

4. COMPRENDRE LE DÉROULEMENT D'UN PAIEMENT

La procédure d'un paiement en ligne s'appréhende de manière différente du point de vue de l'acheteur et du marchand.

4.1. Définir les étapes d'un paiement - Vue acheteur

Cinématique des échanges du point de vue de l'acheteur :



1. L'acheteur valide son panier.
2. Le site marchand redirige l'acheteur vers la plateforme de paiement via un formulaire HTML POST sécurisé en HTTPS.

   Les paramètres à inclure dans ce formulaire sont détaillés dans le chapitre Générer un formulaire de paiement.
3. La plateforme de paiement, après vérification des paramètres et de leur signature, présente le parcours de paiement à l'acheteur.

   Il existe deux parcours selon comment vous avez renseigné le formulaire de paiement :

   - Parcours 1 : Vous avez spécifié un seul moyen de paiement (ex. carte bancaire). La plateforme affiche directement la page de saisie des données du moyens de paiement (étape 5)
   - Parcours 2 : Vous avez spécifié tous vos moyens de paiement disponibles. La plateforme affiche la page de sélection du moyen de paiement.

     Exemple :

Tous droits réservés

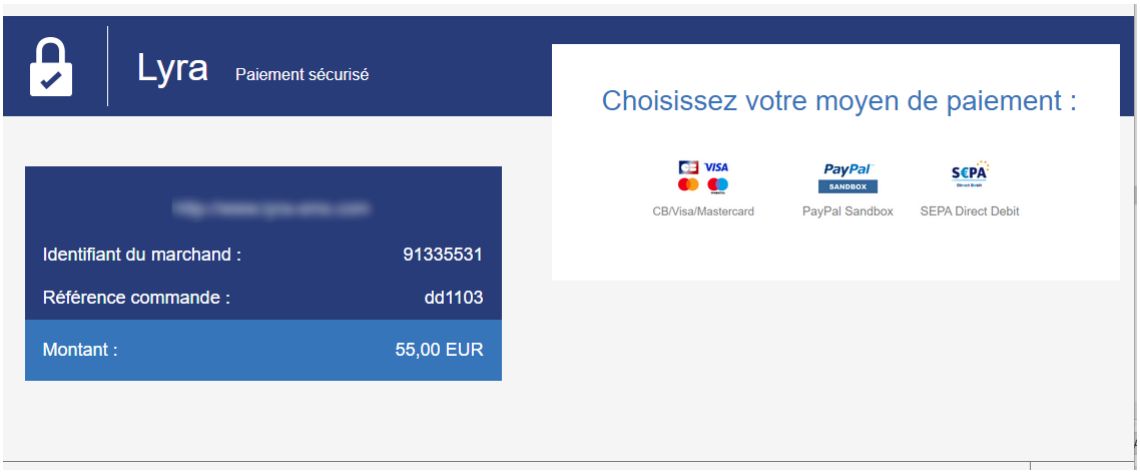


Image 1 : Sélection du moyen de paiement

Un dispositif appelé logo unique regroupe CB, Visa et Mastercard.

Il permet à l'acheteur d'accéder directement sur la page de saisie des données de carte si le marchand possède uniquement un contrat CB.

Dans ce cas de figure, les cartes CB, e-Carte bleue, Visa, Visa Electron, Mastercard et Maestro sont affichés sous un seul logo sur la page de paiement.

4. L'acheteur sélectionne son moyen de paiement si la plateforme affiche le parcours 2.
5. L'acheteur renseigne le numéro et la date d'expiration de sa carte.

   Si la carte possède un cryptogramme visuel, ce dernier doit obligatoirement être renseigné.

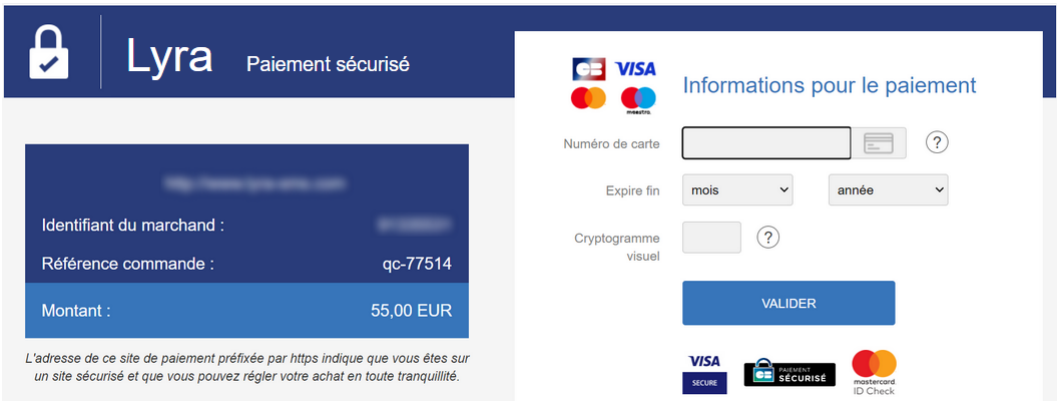


Image 2 : Saisie des informations du moyen de paiement

6. L'acheteur renseigne les informations requises par l'acquéreur, comme :
   - Le nom du titulaire de la carte
7. L'acheteur clique sur **Valider**.

> Une vérification supplémentaire de sécurité se fait à ce niveau si vous avez activé le CAPTCHA sur votre boutique. Consultez le manuel d'utilisation "Gestion des paramétrages de la boutique".
>
> Le CAPTCHA est un test informatique permettant de différencier une action réalisée par un utilisateur humain d'un robot. La vérification est automatique, sans interaction visuelle.
>
> En cas de doute, le CAPTCHA s'affiche et l'acheteur devra répondre en saisissant un texte ou des icônes requises avant de pouvoir valider le paiement.

8. Si le marchand et la carte de l'acheteur sont inscrits à 3-D Secure, une authentification 3-D Secure a lieu.
9. La plateforme effectue des contrôles anti-fraude et envoie une demande d'autorisation à la banque de l'acheteur.
10. Si l'autorisation est acceptée, l'acheteur voit un récapitulatif de la transaction.

Tous droits réservés

Un bouton permettant un retour à la boutique est proposé.

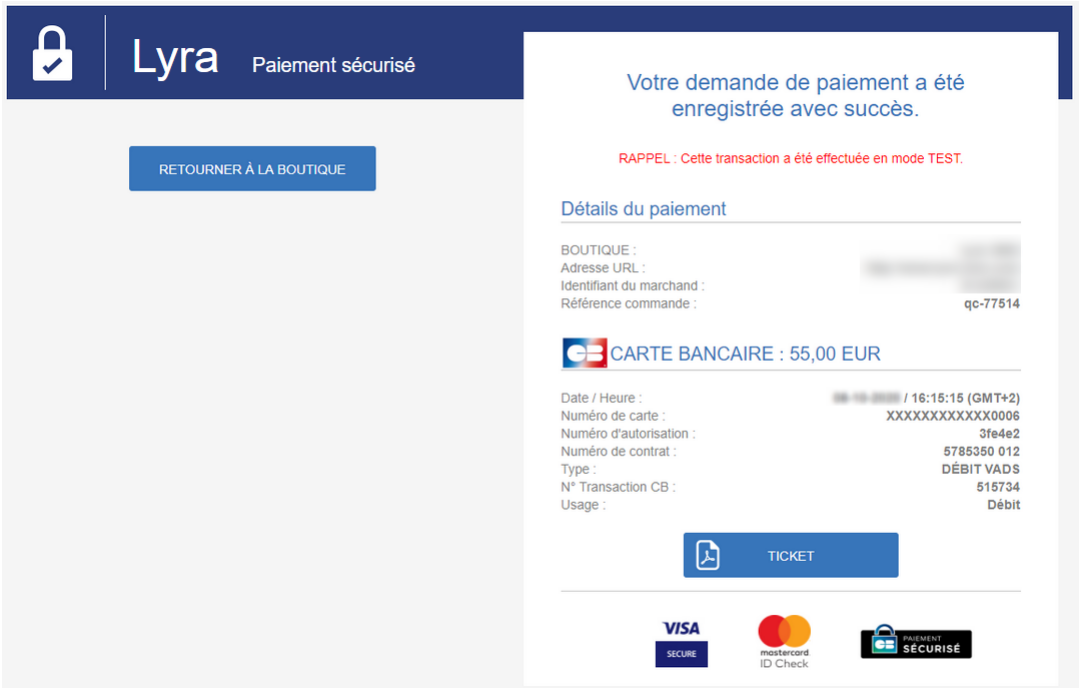


Image 3 : Récapitulatif de la transaction

En cas d'échec, la plateforme informe l'acheteur et affiche un bouton pour annuler et retourner à la boutique.

Si des tentatives supplémentaires sont configurées dans votre Back Office Expert, l'acheteur peut réessayer. Le processus de paiement reprend alors à la sélection du moyen de paiement.

Lorsque toutes les tentatives sont épuisées, le paiement est définitivement refusé.

Image 4 : Page de résumé en cas d'échec de la transaction

Tous droits réservés

4.2. Définir les étapes d'un paiement - Vue marchand

Le paiement en ligne côté marchand suit ces étapes :

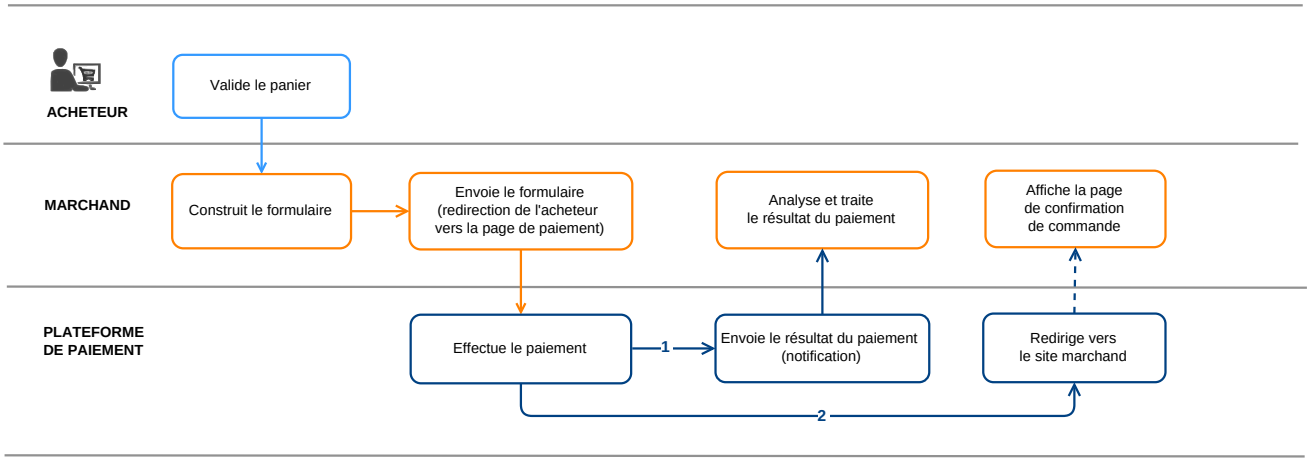


Image 5 : Cinématique des échanges – Vue marchand

1. L'acheteur valide son panier.
2. Le site marchand construit le formulaire à partir des données du panier de l'acheteur.
3. Le site marchand redirige l'acheteur vers la plateforme de paiement via un formulaire HTML POST en HTTPS. Les paramètres sont décrits dans le chapitre Générer un formulaire de paiement.
4. L'acheteur saisit ses informations de paiement, et la plateforme procède au paiement.
5. La plateforme informe automatiquement le site marchand du résultat (selon la configuration), voir chapitre Paramétrer les notifications.
6. Le site marchand analyse et traite le résultat du paiement.
7. Le marchand met à jour sa base de données (état de la commande, état du stock, etc.).
8. L'acheteur est informé du résultat et peut revenir sur le site marchand pour voir l'état de sa commande.

Tous droits réservés

5. PROPOSER DES TENTATIVES DE PAIEMENT SUPPLÉMENTAIRES

Configuration du nombre de tentatives supplémentaires en cas de refus de paiement :

1. Menu **Paramétrage** > **Boutique**, sélectionnez la boutique où la configuration doit être modifiée.
2. Sélectionnez l'onglet **Configuration**.
3. Renseignez le nombre de tentatives supplémentaires autorisées.

   Exemple : 2 tentatives équivaut à 3 essais au total.
4. Cochez **URL de notification sur tentative refusée** si vous souhaitez recevoir une notification (IPN) à chaque refus.
5. Cliquez sur **Sauvegarder**.

Les tentatives supplémentaires ne s'appliquent pas aux paiements en plusieurs fois.

Tous droits réservés

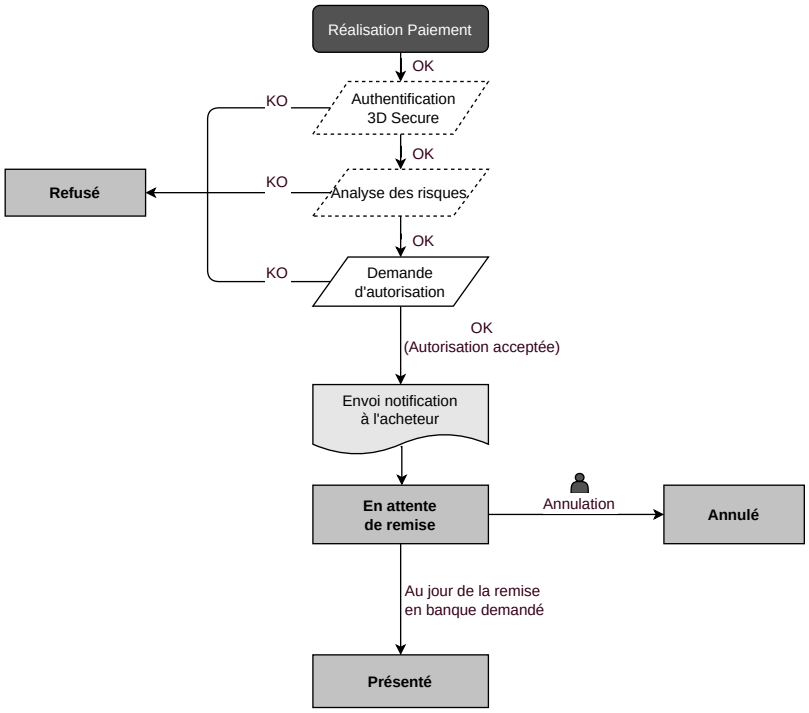
6. CYCLE DE VIE DES TRANSACTIONS

Dans tous les schémas suivants, la légende suivante est adoptée :

Action du marchand nécessaire - manuelle (Back Office Expert) ou automatique (Web Services)

6.1. Paiement comptant immédiat

6.1.1. Validation automatique



Suite à la demande de paiement, plusieurs contrôles sont automatiquement mis en oeuvre :

- L'authentification 3-D Secure.
- Différents contrôles réalisés par la plateforme de paiement (ceux-ci incluent potentiellement les contrôles locaux, les règles de risques configurées par le marchand) ou par un analyseur de risque externe.
- Une demande d'autorisation est également effectuée auprès de la banque de l'acheteur, le jour même de la date de paiement, quelle que soit la date de remise en banque demandée.

Si l'un de ces contrôles échoue, la demande de paiement n'est pas acceptée. L'acheteur est informé du refus à l'écran. Dans le Back Office Expert, la transaction est consultable avec le statut **Refusé**.

Dans le cas contraire, la transaction prend le statut **En attente de remise**.

L'acheteur est informé de l'acceptation de sa demande de paiement et est destinataire d'un e-mail de confirmation.

La transaction partira automatiquement en remise le jour demandé par le marchand et prendra le statut **Présenté**. Le statut **Présenté** est définitif.

Une fois la remise effectuée, la compensation de la transaction sur le compte du marchand dépend des délais de traitements interbancaires.

Dans l'attente de cette remise, le marchand peut modifier la date de remise ainsi que le montant (modification du montant uniquement à la baisse, ce cas correspond à une livraison partielle par le marchand).

Tous droits réservés

Si nécessaire, il peut également annuler la transaction : celle-ci prend alors le statut **Annulé**.

6.1.2. Validation manuelle

Lorsqu'une demande de paiement est initiée, les contrôles suivants sont automatiquement mis en œuvre :

- Authentification3-D Secure.
- Contrôles par la plateforme de paiement.

  Inclut les contrôles locaux et les règles de risque définies par le marchand. Cela peut également impliquer un analyseur de risque externe.
- Demande d'autorisation auprès de la banque de l'acheteur.

En cas d'échec, si l'un des contrôles échoue, la demande de paiement est rejetée. L'acheteur est immédiatement informé du refus sur l'écran, et la transaction est visible dans le Back Office Expert avec le statut **Refusé**.

Si tous les contrôles sont validés, le paiement est accepté. La transaction devient consultable dans le Back Office Expert avec le statut **À valider**.

Le marchand doit alors obligatoirement valider la transaction avant la date d'expiration de la demande d'autorisation. Si cette validation n'est pas effectuée à temps, la transaction passe au statut **Expiré** et ne peut plus être remise en banque.

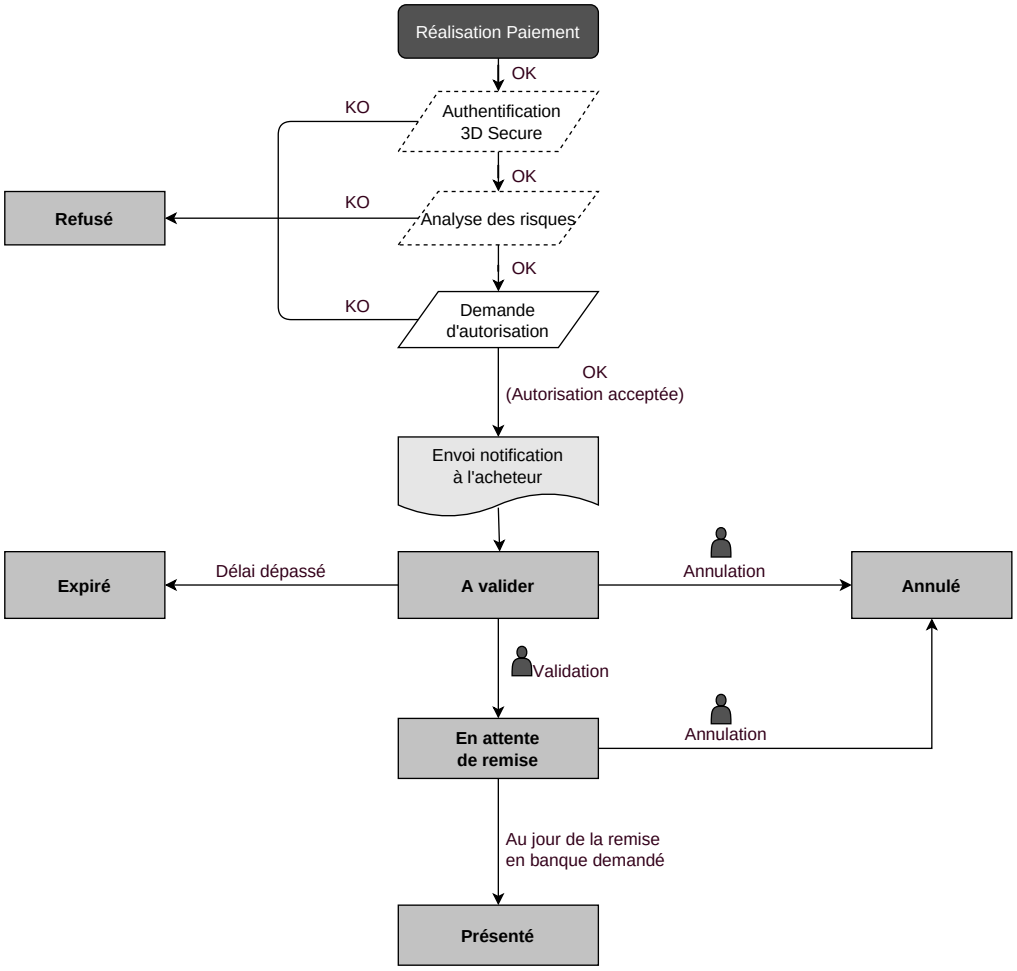
Lorsque le marchand valide une transaction, elle passe en statut **En attente de remise**.

La transaction est automatiquement envoyée en remise à la date défini par le marchand et prendra le statut **Présenté**. Le statut **Présenté** est définitif.

Une fois la remise effectuée, la compensation de la transaction sur le compte du marchand dépend des délais de traitements interbancaires.

Le marchand peut annuler la transaction si nécessaire. La transaction prend le statut **Annulé**.

Tous droits réservés



Tous droits réservés

6.2. Paiement comptant différé

6.2.1. Validation automatique

Délai de remise inférieur à la durée de validité de l'autorisation

(voir diagramme cycle de vie d'une transaction de paiement comptant immédiat).

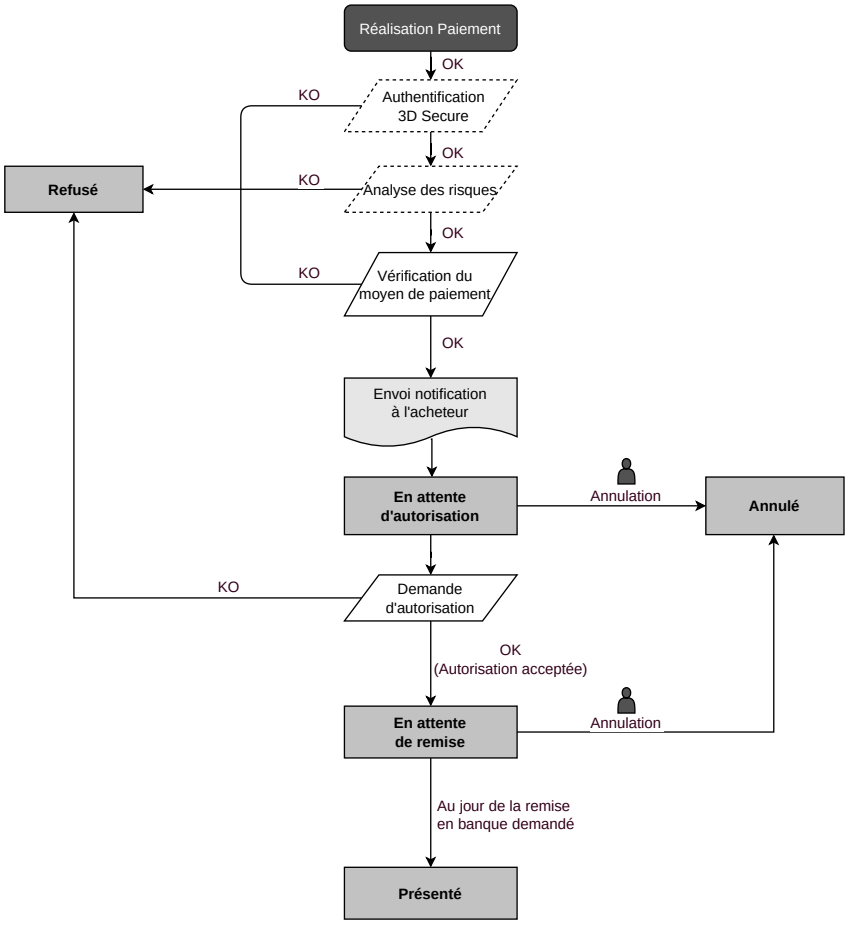
Délai de remise supérieur à la durée de validité de l'autorisation

Toute transaction de paiement comptant différé réalisée avec le mode de validation automatique, et ayant réussi la demande de vérification, est consultable dans le Back Office Expert avec le statut **En attente d'autorisation**.

La demande d'autorisation est automatiquement effectuée :

- Fonctionnement par défaut : la veille de la date de remise en banque souhaitée,
- Fonctionnement avec autorisation anticipée : selon le moyen de paiement sélectionné, plusieurs jours avant la date de remise en banque souhaitée (voir chapitre Le service "Autorisations anticipées" à la page 19).

Le diagramme suivant résume les différents statuts d'un paiement différé :



6.2.2. Validation manuelle

Délai de remise inférieur à la durée de validité de l'autorisation

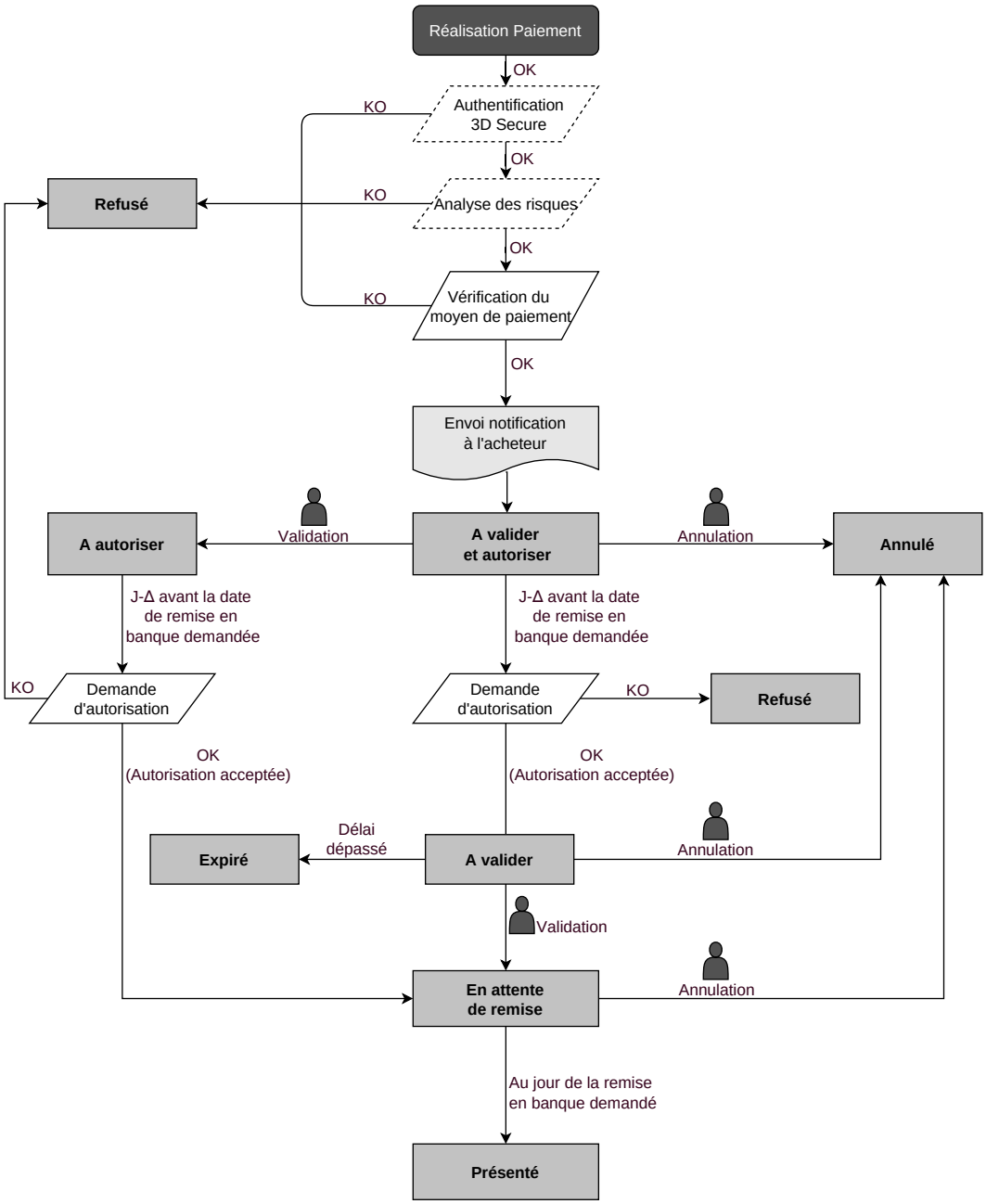
(voir diagramme cycle de vie d'une transaction de paiement comptant immédiat).

Délai de remise supérieur à la durée de validité de l'autorisation

Toute transaction de paiement comptant différé réalisée avec le mode de validation manuelle et dont la demande d'autorisation à 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte) a été réalisée avec succès, est consultable dans le Back Office Expert avec le statut **À valider et autoriser**.

La demande d'autorisation est automatiquement effectuée le jour de la remise en banque demandé, sous réserve que le marchand ait validé la transaction.

Dans l'attente de la remise, le marchand peut annuler la transaction ou modifier le montant ainsi que la date de remise en banque. Ces transactions suivent le diagramme d'état suivant :



Tous droits réservés

6.3. Paiement en plusieurs fois

6.3.1. Validation automatique

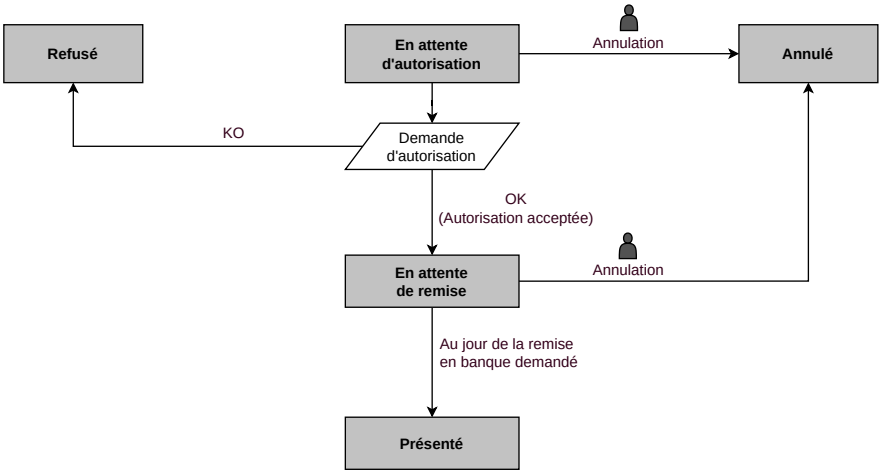
La première échéance du paiement en plusieurs fois se comportera exactement comme une transaction de paiement comptant immédiat ou une transaction de paiement différé selon sa date de remise en banque.

Les échéances suivantes sont par défaut en statut **En attente d'autorisation**. La banque de l'acheteur peut refuser la demande d'autorisation. En cas de refus, la plateforme de paiement informe le marchand par e-mail.

Les demandes d'autorisation des échéances suivantes sont automatiquement traitées comme des transactions de paiement différé. Deux dates possibles :

- Par défaut, l'autorisation est demandée la veille de la date de remise en banque souhaitée.
- Avec l'autorisation anticipée, selon le moyen de paiement sélectionné, l'autorisation est effectuée plusieurs jours avant la date de remise en banque souhaitée (voir chapitre Le service "Autorisations anticipées" à la page 19).

Les échéances ultérieures suivent le diagramme d'état suivant (cas d'une demande d'autorisation non rejouée) :



L'annulation d'une échéance n'implique en aucun cas l'annulation des échéances suivantes restant à remettre en banque.

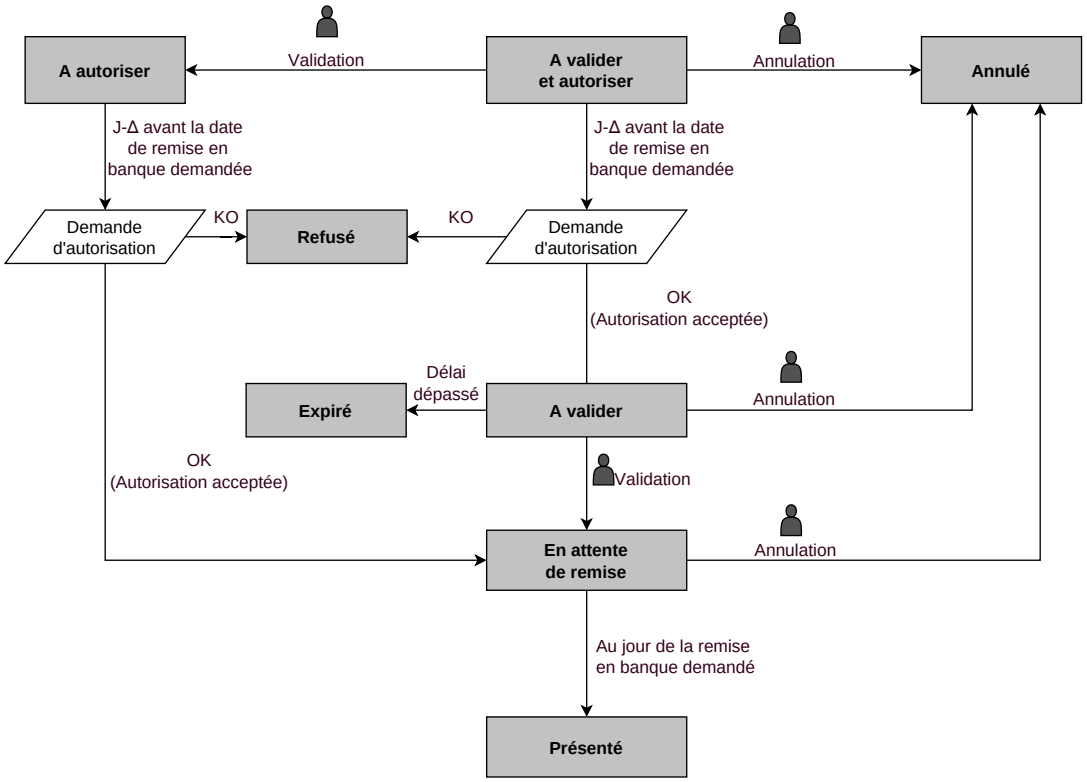
Tous droits réservés

6.3.2. Validation manuelle

La première échéance d'un paiement en plusieurs fois suit le comportement d'une transaction de paiement comptant immédiat ou différé, en fonction de la date de remise en banque demandée.

Les échéances suivantes sont par défaut positionnées en statut **À valider et autoriser** tant que la première échéance n'a pas été validée par le marchand. Cependant, leur bonne exécution n'est pas garantie, car la banque de l'acheteur peut refuser une demande d'autorisation.

La validation de la première échéance équivaut à la validation automatique de toutes les échéances suivantes. En revanche, l'annulation d'une échéance n'entraîne pas l'annulation des échéances ultérieures.



Tous droits réservés

7. 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.

7.1. Définir l'URL de la page de paiement

Le site marchand communique avec la plateforme de paiement en redirigeant l'acheteur vers l'URL ci-dessous.

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

7.2. S'identifier lors des échanges

Pour dialoguer avec la plateforme de paiement, le marchand a besoin de deux informations :

- L'identifiant boutique : Il permet d'identifier le site marchand lors des échanges avec la plateforme. Sa valeur est transmise dans le champ **vads_site_id.**
- La clé: Elle permet de calculer la signature alphanumérique transmise dans le champ **signature**.

Pour récupérer ces valeurs :

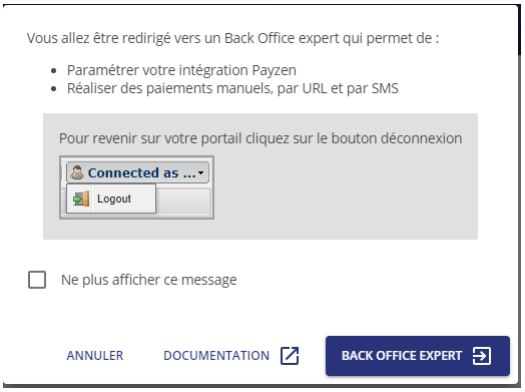
1. Connectez-vous à votre **Back Office Lyra Collect** : https://secure.lyra.com/portal/
2. Saisissez votre nom d'utilisateur.
3. Saisissez votre mot de passe.
4. Cliquez sur **Connexion**.

   En cas d'erreur de saisie du nom d'utilisateur et/ou du mot de passe, le message d'erreur "*Nom d'utilisateur ou mot de passe invalide*" s'affiche.

   Vous pouvez corriger votre saisie ou cliquer sur le lien **Mot de passe oublié ou compte bloqué**.
5. Cliquez sur **Autres actions**.

   La fenêtre suivante s'affiche :

Tous droits réservés



6. Cliquez sur **Back Office Expert** pour accéder à votre Back Office Expert

7. Cliquez sur **Paramétrage > Boutique**.

8. Sélectionnez l'onglet **Clés**.

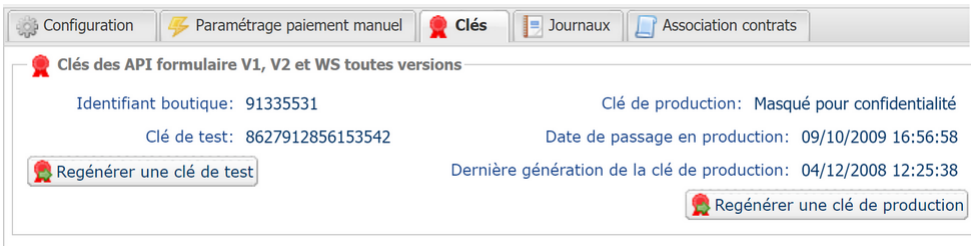


Image 6 : Onglet Clés

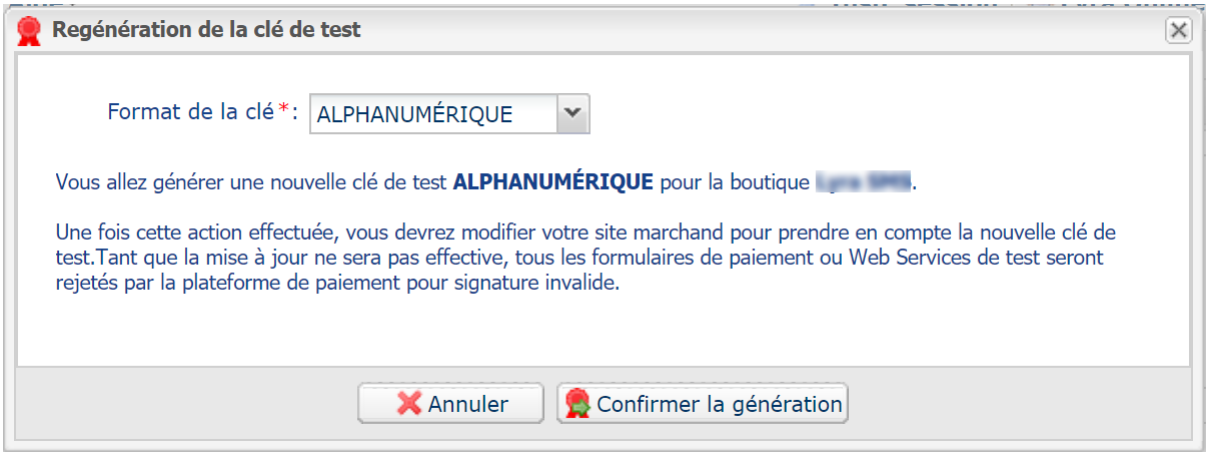
Deux types de clé sont mis à disposition :

- La clé de test : elle est utilisée pour générer la signature d'un formulaire en mode test.
- La clé de production : elle est utilisée pour générer la signature d'un formulaire en mode production.

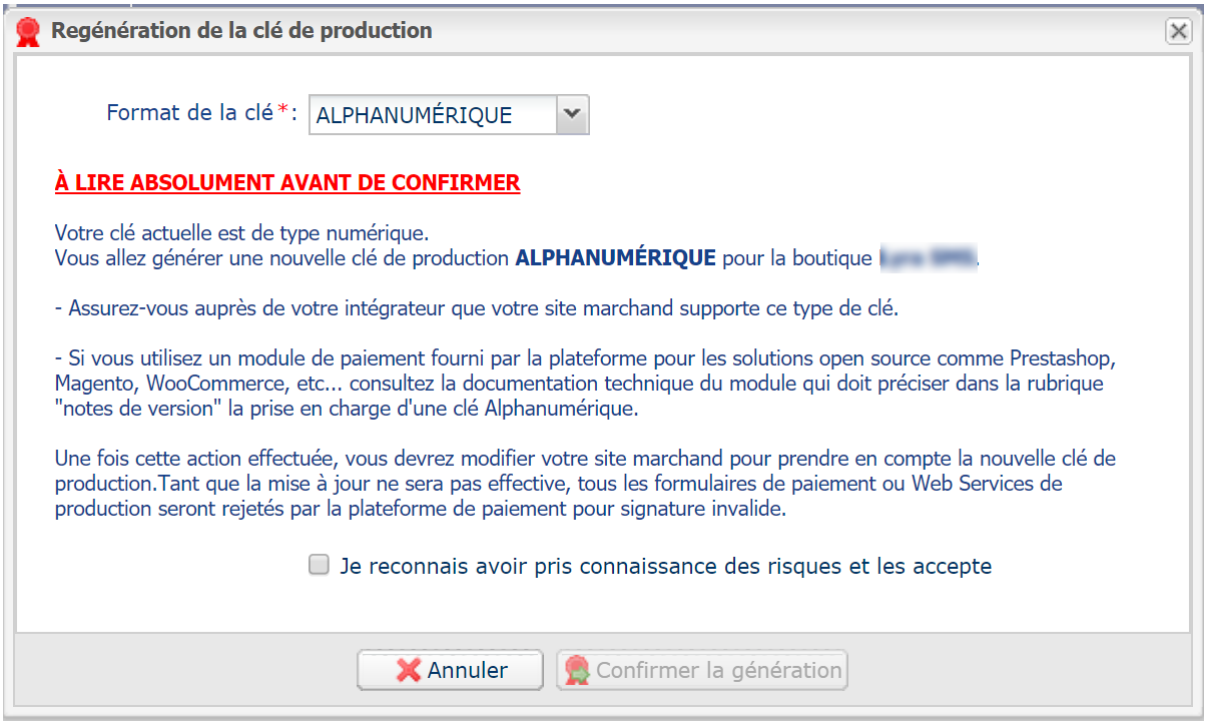
Ces clés peuvent être numériques ou alphanumériques.

Pour un maximum de sécurité, il est recommandé d'utiliser une clé alphanumérique.

Pour modifier le format de votre clé de test, cliquez sur le bouton **Régénérer une clé de test**, puis sélectionnez le format (ALPHANUMERIQUE ou NUMERIQUE).



Pour changer le format de votre clé de production, cliquez sur le bouton **Régénérer une clé de production**, puis sélectionnez ALPHANUMERIQUE ou NUMERIQUE).



7.3. Choisir le mode Test ou Production

Le choix du mode TEST ou PRODUCTION se fait avec le champ **vads_ctx_mode** (Voir chapitre Générer un formulaire de paiement à la page 63).

- Le mode TEST permet de réaliser des paiements de test sans créer de transactions réelles.

  Il reste disponible après la génération de la clé de production.

  Les tests réalisés sur un nouveau site marchand ou un environnement de recette n'affectent pas le site en production. Les transactions de TEST sont consultables dans le Back Office Expert via Gestion > Transactions de TEST.

- Le mode **PRODUCTION**

  s'active après la génération de la clé de production et permet de traiter des paiements réels.

  .

  Les transactions de PRODUCTION sont visibles dans le Back Office Expert via **Gestion** > **Transactions**.

7.4. Gérer le dialogue vers le site marchand

Le dialogue avec le site marchand utilise deux types d'URL :

- **URL de notification instantanée**, également appelée IPN (Instant Payment Notification),
- **URL de retour** vers le site marchand.

URL de notification instantanée - IPN (Instant Payment Notification) :

L'**URL de notification** correspond à une page dédiée sur le site marchand. La plateforme de paiement l'appelle automatiquement lorsqu'un événement spécifique se produit.

Par défaut des règles sont créées pour gérer les événements suivants :

- Fin d'un paiement (accepté ou refusé),
- Abandon ou annulation durant le paiement,
- Création ou mise à jour d'un alias,
- Création d'un abonnement,
- Nouvelle échéance d'un abonnement,
- Autorisation réalisée dans le cas d'un paiement différé,
- Modification du statut d'une transaction par l'acquéreur,
- Opération réalisée depuis le Back Office Expert (annulation, remboursement, duplication, paiement manuel, etc..).

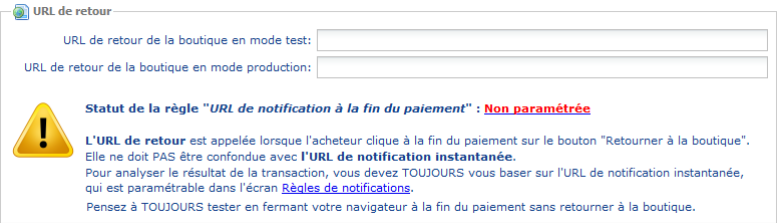
Ces règles doivent être activées et convenablement configurées en fonction des besoins du marchand.

A chaque appel, la plateforme de paiement transmet au site marchand les données relatives à une transaction. C'est ce qu'on appelle une notification instantanée (ou **IPN** pour Instant Payment Notification).

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.

URL de retour vers le site marchand

Le marchand peut paramétrer dans le Back Office Expert les URL de retour "par défaut" depuis le menu **Paramétrage** > **Boutique** > onglet **Configuration** :



Il peut configurer une URL de retour à la boutique différente en fonction du mode.

Par défaut, l'acheteur est redirigé vers l'URL de retour, et ce, quel que soit le résultat du paiement.

Si toutefois aucune URL n'est configurée à ce niveau, alors la redirection utilisera l'URL principale de la boutique (paramètre **URL** défini dans l'encadré **Détails** de la boutique).

Le marchand a la possibilité de surcharger cette configuration dans son formulaire de paiement (voir chapitre **Définir les URL de retour**).

Le statut de la règle "URL de notification à la fin du paiement" (IPN) est affiché dans cet écran. Si cette dernière est non paramétrée, veillez à la renseigner (voir chapitre **Paramétrer les notifications**).

Tous droits réservés

7.5. Gérer la sécurité

Plusieurs moyens sont mis en place afin d'assurer la sécurité des transactions de paiement en ligne.

7.5.1. Garantir l'intégrité des échanges

L'intégrité des informations échangées est garantie par un échange de signatures alphanumériques entre la plateforme de paiement et le site marchand.

Le dialogue entre les deux parties se fait via des formulaires HTML.

Un formulaire contient une liste de champs spécifiques (voir chapitre "Générer un formulaire de paiement") utilisés pour générer une chaîne.

Cette chaîne est réduite à une taille inférieure grâce à une fonction de hachage (SHA-1, HMAC-SHA-256).

Le marchand sélectionne l'algorithme de hachage dans son Back Office Expert (voir chapitre "Sélectionner l'algorithme de hachage").

La chaîne résultante, appelée empreinte, est ensuite transmise dans le champ **signature** (voir le chapitre "Calculer la signature")

Modélisation des mécanismes de sécurité :

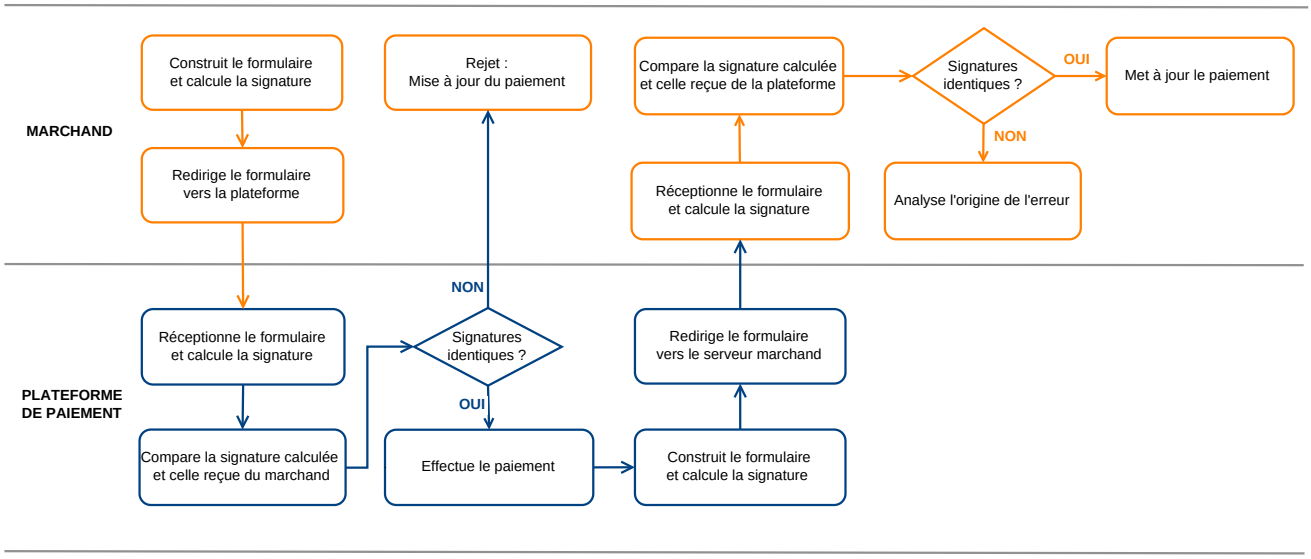


Image 7 : Diagramme mécanisme de sécurité

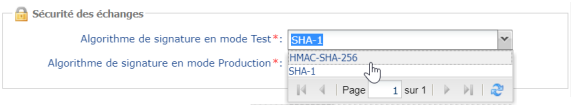
1. Le site marchand construit les données du formulaire et calcule la signature.
2. Le site marchand envoie le formulaire à la plateforme.
3. La plateforme reçoit les données et calcule la signature avec les données reçues.
4. La plateforme compare cette signature à celle transmise par le site marchand.
5.
   - Si les signatures diffèrent, la demande de paiement est rejetée.
   - Sinon, la plateforme procède au paiement.
6. La plateforme construit les données de la réponse et calcule la signature.
7. Selon le paramétrage de la boutique (voir chapitre "Paramétrer les notifications"), la plateforme envoie le résultat du paiement au site marchand.

Tous droits réservés

8. Le site marchand reçoit les données et calcule la signature. Il la compare à celle transmise par la plateforme.
9.
   - Si les signatures diffèrent, le marchand analyse l'origine de l'erreur (calcul incorrect, tentative de fraude etc.)
   - Sinon, le site marchand met à jour sa base de données (état du stock, statut de la commande etc.).

7.5.2. Sélectionner l'algorithme de hachage

Depuis le Back Office Expert (menu **Paramétrage** > **Boutique** > **Clés**), le marchand peut choisir la fonction de hachage pour générer les signatures.



Par défaut, c'est l'algorithme HMAC-SHA-256 qui sera appliqué.

Vous pouvez sélectionner un algorithme différent pour le mode Test et le mode Production.

Cependant, assurez-vous d'utiliser la même méthode pour générer vos formulaires de paiement et analyser les données reçues lors des notifications de la plateforme de paiement.

Pour faciliter le changement d'algorithme, les signatures en SHA-1 ou en HMAC-SHA-256 sont acceptées sans générer de rejet pour erreur de signature pendant 24 heures.

7.5.3. Conserver la clé de production

Dès le premier paiement avec une carte réelle, la clé de production est masquée pour des raisons de sécurité.

Conservez cette clé dans un emplacement sécurisé (fichier chiffré, base de données etc.).

En cas de perte, vous pouvez générer une nouvelle clé depuis le Back Office Expert.

La clé de production est accessible dans le Back Office Expert depuis le menu **Paramétrage** > **Boutique** > onglet **Clés**.

7.5.4. Gérer les données sensibles

Les transactions de paiement en ligne sont soumises à des règles strictes (Certification PCI-DSS).

Bonnes pratiques pour les marchands :

- Ne jamais enregistrer ou transmettre en clair des données pouvant ressembler à un numéro de carte bancaire.

  Un formulaire contenant de telles données sera rejeté avec le code *999 - Sensitive data detected*.
- Évitez les numéros de commande entre 13 et 16 chiffres commençant par 3, 4 ou 5, car ils pourraient être interprétés comme des numéros de carte bancaire.

Tous droits réservés

7.6. Gérer les paramètres de votre boutique avec un fichier de configuration

Un fichier de configuration permet d'éviter de mettre des valeurs directement dans le code.

Contenu des fichiers de configuration :

- L'URL de la page de paiement,
- Les clés de test et de production,
- L'identifiant de la boutique,
- Permet de typer les données,
- Facilite l'interrogation par le programme pour récupérer les paramètres nécessaires à la génération des formulaires de paiement.

Restreignez l'accès au fichier de configuration avec des solutions comme un fichier *.htaccess* ou des réécritures d'URL.

Exemple de fichier de configuration "conf.txt" :

```
vads_site_id = 11111111
TEST_key = 2222222222222222
PROD_key = 3333333333333333
vads_ctx_mode = TEST
```

Exemple d'appel de fichier de configuration dans le formulaire de paiement :

```
$conf_txt = parse_ini_file("conf.txt");
 if ($conf_txt['vads_ctx_mode'] == "TEST") $conf_txt['key'] = $conf_txt['TEST_key'];
 if ($conf_txt['vads_ctx_mode'] == "PRODUCTION") $conf_txt['key'] = $conf_txt['PROD_key'];
```


Tous droits réservés

8. PARAMÉTRER LES NOTIFICATIONS

Le Back Office Expert permet de gérer les événements déclenchant l'envoi d'une notification vers le site marchand et de configurer l'URL de la page à contacter.

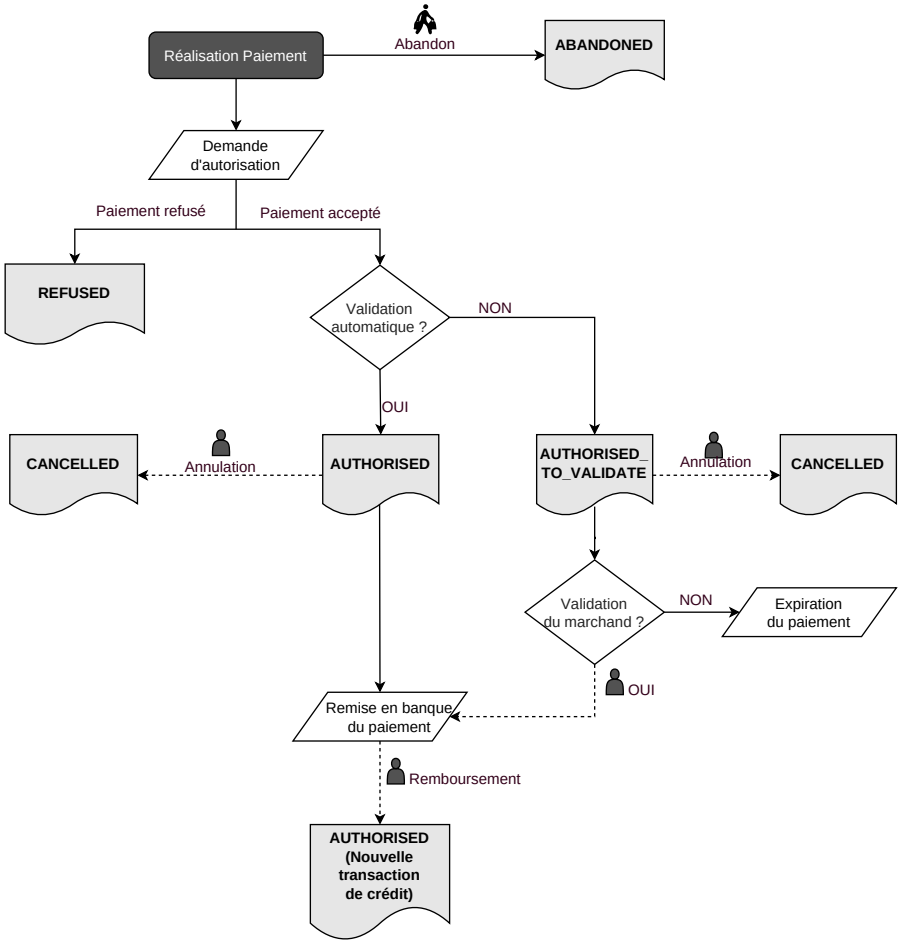
Les schémas suivants illustrent pour chaque événement le statut de transaction envoyé dans la notification.

La légende adoptée pour chacun est la suivante :

Action du marchand nécessaire, manuelle (Back Office Expert) ou automatique (API Web service)

Action de l'acheteur

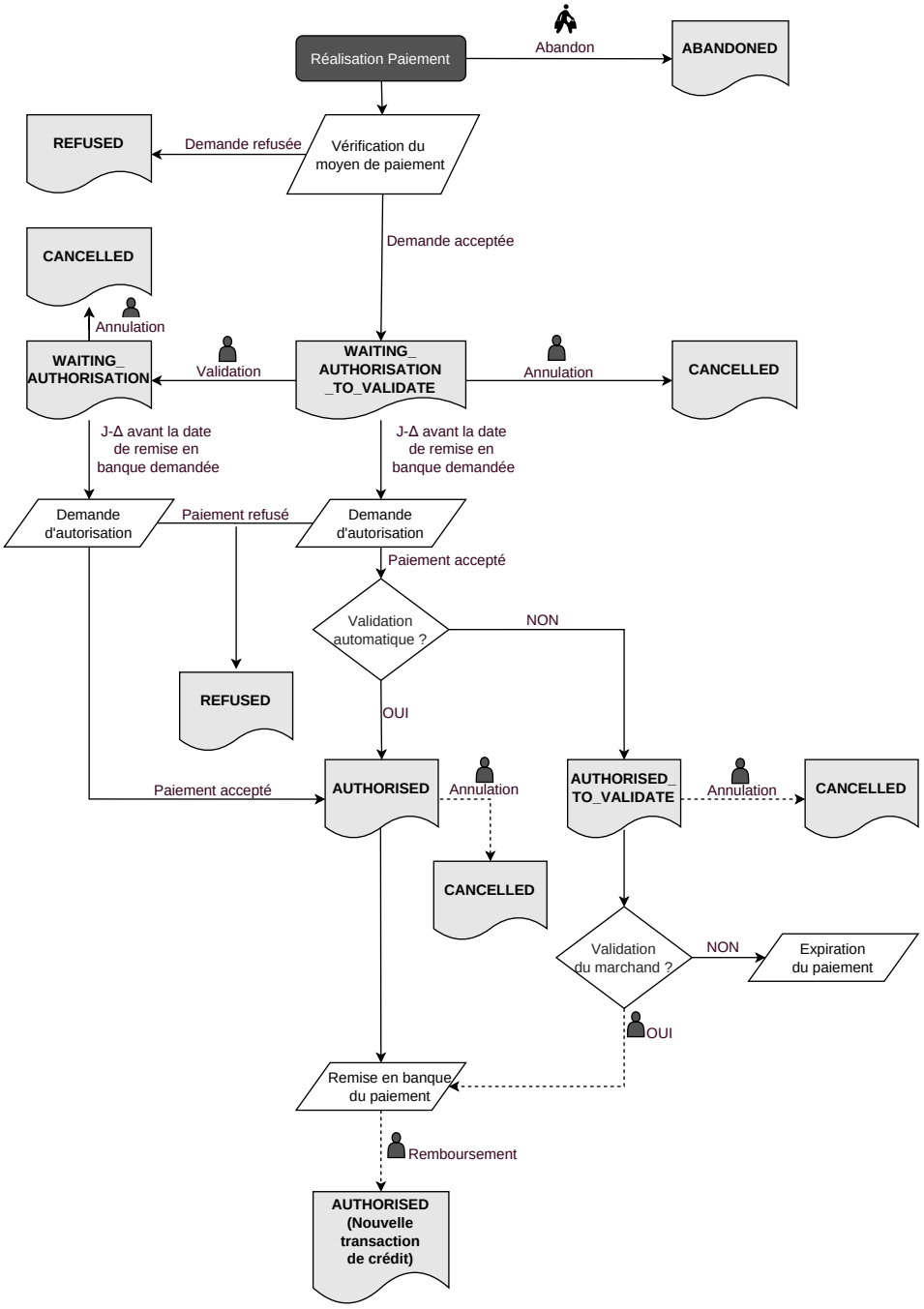
8.1. Notifications des différents statuts pour un paiement comptant immédiat



Evénement	Statut notifé	Nom de la règle à paramétrer
Abandon par l'acheteur	ABANDONED	URL de notification sur annulation
Annulation par le marchand	CANCELLED	URL de notification sur une opération provenant du Back Office
Réponse à la demande d'autorisation	AUTHORISED_TO_VALIDATE, AUTHORISED, REFUSED	URL de notification à la fin du paiement

Tous droits réservés

8.2. Notifications des différents statuts pour un paiement comptant différé

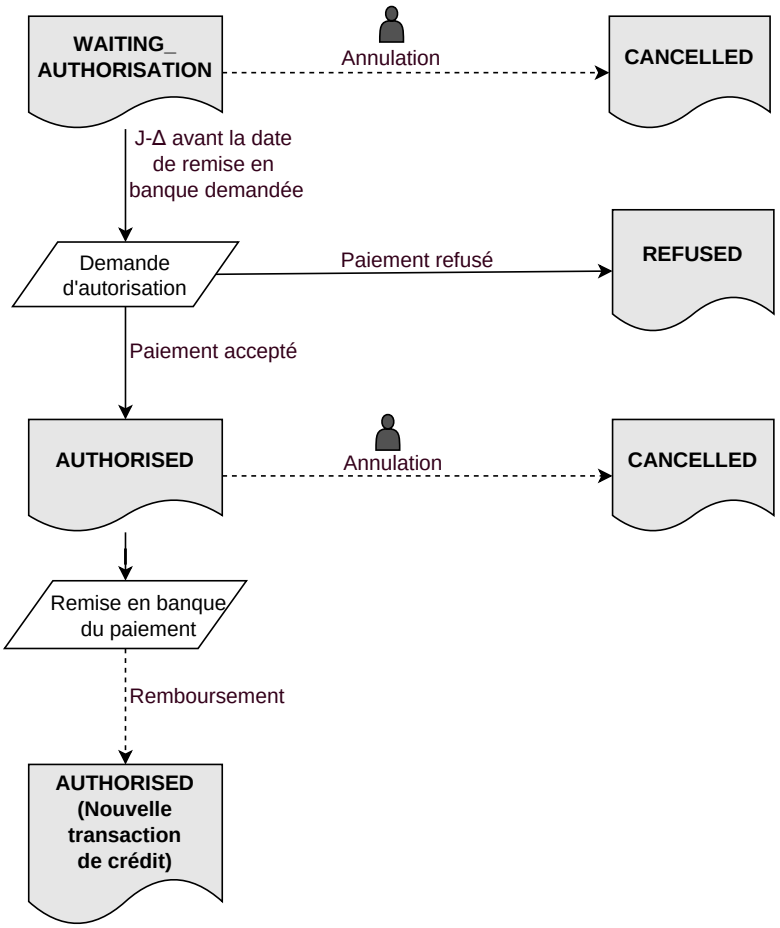


Δ : durée de validité d'autorisation.

Evénement	Statut notifé	Nom de la règle à paramétrer
Abandon par l'acheteur	ABANDONED	URL de notification sur annulation
Annulation par le marchand	CANCELLED	URL de notification sur une opération provenant du Back Office
Validation par le marchand	WAITING_AUTHORISATION	URL de notification sur une opération provenant du Back Office

Evénement	Statut notifé	Nom de la règle à paramétrer
Réponse à la demande d'autorisation à 1 EUR (ou demande de renseignement sur le réseau CB si l'acquéreur le supporte)	REFUSED, WAITING_AUTHORISATION, WAITING_AUTHORISATION_TO_VALIDATE	URL de notification à la fin du paiement
Réponse à la demande d'autorisation	AUTHORISED, REFUSED, AUTHORISED_TO_VALIDATE	URL de notification sur autorisation par batch

8.3. Notifications des différents statuts pour les échéances d'un paiement en plusieurs fois



Δ : durée de validité d'autorisation.

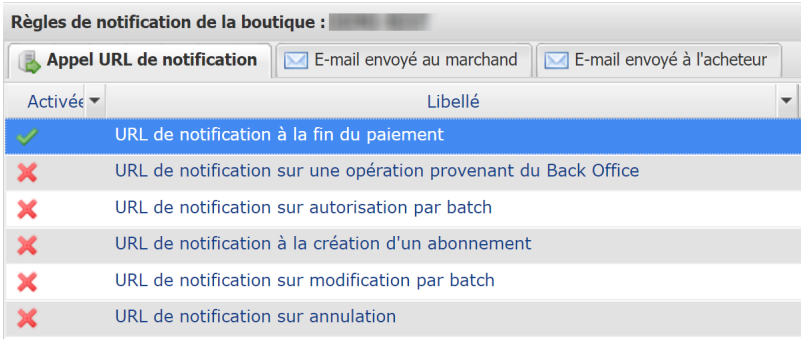
Evénement	Statut notifé	Nom de la règle à paramétrer
Annulation par le marchand	CANCELLED	URL de notification sur une opération provenant du Back Office
Réponse à la demande d'autorisation	AUTHORISED, REFUSED	URL de notification sur autorisation par batch

Tous droits réservés

8.4. Accéder au centre de notification

Ouvrez le menu **Paramétrage** > **Règles de notifications**.

L'onglet de configuration des règles de type **Appel URL de notification** s'affiche.



8.5. 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.

L'événement **Paiement accepté** correspond à la création d'une transaction dans l'un des statuts (`vads_trans_status`) ci-dessous :

- **ACCEPTED**
- **AUTHORISED**
- **AUTHORISED_TO_VALIDATE**
- **CAPTURED**
- **INITIAL**
- **UNDER_VERIFICATION**
- **WAITING_AUTHORISATION**
- **WAITING_AUTHORISATION_TO_VALIDATE**
- **WAITING_FOR_PAYMENT**

Cette notification est indispensable pour transmettre le résultat d'une demande de paiement.

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

1. Faites 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 **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 59.

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.

Tous droits réservés

8.6. Configurer la notification sur autorisation par batch

Cette notification est indispensable pour communiquer le résultat d'un paiement différé :

- En cas de paiement accepté.
- En cas de paiement refusé.

Elle permet au site marchand d'être notifié lorsque la demande d'autorisation n'est pas réalisée le jour du paiement.

Exemple :

Pour un paiement différé avec un délai de remise à 60 jours, la demande d'autorisation n'est pas faite lors du paiement. Le site marchand sera contacté lors de la demande d'autorisation par la règle **URL de notification sur autorisation par batch**.

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 **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 59.
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**.

Tous droits réservés

8.7. 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 59.
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**.

Tous droits réservés

8.8. 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 59.
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

8.9. Configurer la notification sur modification par batch

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

- Lorsqu'une transaction expire.

  Cela concerne les transactions créées en validation manuelle et non validées à temps par le marchand. Le statut passe à "Expiré" (EXPIRED).

- Lorsqu'une transaction **PayPal**, bloquée pour suspicion de fraude, est acceptée ou refusée.

  Le statut des transactions concernées passe de "Vérification en cours" (UNDER_VERIFICATION) à "Présenté" (CAPTURED) ou "Refusé" (REFUSED).

- Lorsqu'une transaction **3x 4x Oney** est acceptée après analyse du dossier de financement.
- Lorsqu'une transaction **Franfinance** est acceptée ou refusée.
- Pour les transactions réalisées avec les moyens de paiement suivants :

  Alipay, Bancontact, Giropay, iDeal, Multibanco, MyBank, Przelewy24, UnionPay, WeChat Pay.

Cette règle est désactivée par défaut.

1. Effectuez un clic droit sur la ligne **URL de notification sur modification 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 **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 59.
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 modification par batch** et en sélectionnant **Activer la règle**.

8.10. 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.

8.11. Configurer les e-mails envoyés au marchand

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 au marchand**.
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 et l'adresse à notifier.
   Pour spécifier plusieurs adresses e-mails, séparez-les par un point-virgule.
7. Pour personnaliser le contenu de l'e-mail.
   a. Cliquez sur **Paramétrage e-mail**.
   b. Sélectionnez le modèle d'e-mail à appliquer
   c. Cliquez sur le lien **Personnaliser des valeurs de texte par défaut** pour modifier l'objet et le contenu de l'e-mail par défaut.
   d. Cliquez sur **Champs à inclure** pour afficher la liste des champs disponibles pour personnaliser l'e-mail.

e. 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**.

8.12. 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.

Tous droits réservés

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**.

9. 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`

9.1. Créer un paiement comptant immédiat

En mode paiement comptant immédiat, l'acheteur règle la totalité de son achat en une seule fois.

Le paiement est remis en banque le jour même.

1. Utilisez tous les champs du tableau ci-après pour construire le formulaire de paiement.

Nom du champ	Description	Format	Valeur
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
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_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
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_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_page_action	Action à réaliser	enum	PAYMENT
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
vads_payment_config	Type de paiement	enum	SINGLE
vads_payment_cards	Permet de forcer le type de carte à utiliser. Affichez un bouton de paiement distinct pour chaque moyen de paiement disponible sur le site marchand Il est déconseillé de laisser le champ vide. Consultez le chapitre Gérer les moyens de paiement proposés à l'acheteur à la page 95 pour plus d'informations.	enum	Ex : • CB • CVCONNECT • MASTERCARD • VISA • SDD

Tous droits réservés

Nom du champ	Description	Format	Valeur
vads_capture_delay	Délai avant remise en banque.	n..3	
vads_validation_mode	Mode de validation	n1	**0** (Automatique)
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. Valorisez le champ **vads_payment_config** à **SINGLE**.
3. Valorisez le champ **vads_capture_delay** à **0**.
4. Valorisez le champ **vads_validation_mode** à **0** pour une validation automatique (le paiement sera remis automatiquement à la banque).
5. Valorisez le champ **vads_currency** avec le code de la devise souhaitée en utilisant le tableau des devises.
6. Ajoutez les champs recommandés pour augmenter les chances de frictionless lors du paiement.
7. Ajoutez les champs optionnels en fonction de vos besoins (voir chapitre "Utiliser des fonctions complémentaires".

Exemple de formulaire pour le paiement comptant :

```
<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="15000" />
<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_order_id" value="CX-1254" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_cards" value="CB" />
<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="20190626101407" />
<input type="hidden" name="vads_trans_id" value="pt156G" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="0WaYrONo3L0VZqMcvyVf8vT/g8KfZKJ+1jqiAs3Ehiw="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

9.2. Créer un paiement comptant différé

Un paiement comptant différé est un paiement débité en une seule fois dont le délai de remise en banque est strictement supérieur à 0 jour.

Une demande de renseignement sera réalisée si le délai de remise est supérieur à la durée de validité d'une demande d'autorisation (voir chapitre Durée de validité d'une demande d'autorisation à la page 21).

La demande de renseignement a pour objectif de vérifier la validité de la carte. Pour les acquéreurs ne supportant pas les demandes de renseignements, une demande d'autorisation à 1 EUR est réalisée.

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

Nom du champ	Description	Format	Valeur
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
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_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
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_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_page_action	Action à réaliser	enum	PAYMENT
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
vads_payment_config	Type de paiement	enum	SINGLE
vads_payment_cards	Permet de forcer le type de carte à utiliser. Il est recommandé de proposer sur le site marchand un bouton de paiement différent pour chaque moyen de paiement. **Il est déconseillé de laisser le champ vide**. Consultez le chapitre Gérer les moyens de paiement proposés à l'acheteur à	enum	Ex : • CB • CVCONNECT • MASTERCARD • VISA • SDD

Nom du champ	Description	Format	Valeur
	la page 95 pour plus d'informations.		
vads_capture_delay	Délai avant remise en banque **dont la valeur doit être supérieure à 0**	n..3	Ex :3
vads_validation_mode	Précise le mode de validation de la transaction (manuellement par le marchand, ou automatiquement par la plateforme)	n1	**0** ou **1** ou **absent** ou **vide**
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. Valorisez le champ **vads_payment_config** à **SINGLE**.

3. Valorisez le champ **vads_capture_delay** avec une valeur **supérieure à 0**.

4. Valorisez le champ **vads_validation_mode** à **0** pour une validation automatique (le paiement sera remis de manière automatique à la banque) ou à **1** pour une validation manuelle (le paiement sera remis en banque après une validation manuelle dans le Back Office Expert).

5. Valorisez le champ **vads_currency** avec le code de la devise souhaitée en utilisant le tableau des devises.

6. Ajoutez les champs recommandés pour augmenter les chances de frictionless lors du paiement.

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

Exemple de formulaire de paiement comptant différé :

```
<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="3000" />
<input type="hidden" name="vads_capture_delay" value="3" />
<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_cards" value="CB" />
<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="20190629130025" />
<input type="hidden" name="vads_trans_id" value="Hu92ZQ" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="NrHSHyBBBc+TtcauudspNHQ5cYcy4tS4IjvdC0ztFe8="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

9.3. Créer un paiement en plusieurs fois

Dans le cadre de l'application de la DSP2, une authentification forte est requise lors du paiement de la première échéance. Le champ vads_threeds_mpi est ignoré et la valeur CHALLENGE_MANDATE est appliquée automatiquement.

Ce mode de paiement permet au marchand de proposer une facilité de paiement à l'acheteur.

Le formulaire de paiement définit le nombre d'échéances et l'intervalle qui les sépare.

La première échéance fonctionne de la même manière qu'un paiement comptant immédiat.

La ou les échéances suivantes s'apparentent à un ou des paiements comptant différés.

Des règles de notifications doivent être activées selon l'échéance. Référez-vous au chapitre **Paramétrer les notifications** pour plus de détails.

Le champ **vads_amount** contient le montant total de la commande. C'est ce montant qui sera scindé selon la valeur du champ **vads_payment_config**.

Le jour du paiement, le marchand n'est pas crédité de la totalité du montant et la garantie de paiement ne peut s'appliquer sur les échéances futures.

La date de la dernière échéance ne peut être supérieure à 1 an par rapport à la date de soumission du formulaire. Dans le cas contraire, un message d'erreur est affiché et le formulaire rejeté.

1. Utilisez l'ensemble des champs présents ci-dessous pour construire votre formulaire de paiement.

Nom du champ	Description	Format	Valeur
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
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_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
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_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_page_action	Action à réaliser	enum	PAYMENT

Nom du champ	Description	Format	Valeur
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
vads_payment_config	Type de paiement	enum	voir étape 2.
vads_payment_cards	Permet de forcer le type de carte à utiliser. Affichez un bouton de paiement distinct pour chaque moyen de paiement disponible sur le site marchand. **Il est déconseillé de laisser le champ vide**. Consultez le chapitre Gérer les moyens de paiement proposés à l'acheteur à la page 95 pour plus d'informations.	enum	Ex : • CB • MASTERCARD • VISA
vads_capture_delay	Délai avant remise en banque.	n..3	
vads_validation_mode	Précise le mode de validation de la transaction (manuellement par le marchand, ou automatiquement par la plateforme)	n1	**0** ou **1** ou **absent** ou **vide**
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. Valorisez le champ **vads_payment_config** en respectant la syntaxe suivante:
   - Montants et dates d'échéances fixes :

     MULTI:first=1000;count=3;period=30 où :

     "first" correspond au montant (dans la plus petite fraction de la devise) du premier paiement réalisé le jour du paiement,

     "count" représente le nombre total d'échéances,

     "period" détermine l'intervalle entre chaque échéance.
   - Montants et dates d'échéance personnalisés :

     MULTI_EXT:date1=montant1;date2=montant2;date3=montant3 où :

     date1=montant1 définit la date et le montant du premier versement.

     Les montants sont exprimés dans la plus petite fraction de la devise. La somme dees montants doit être égale à la valeur du champ **vads_amount**.

     Les dates sont exprimées au format YYYYMMDD.
3. Valorisez le champ **vads_capture_delay** à **0** pour que le paiement soit remis en banque le jour même.
4. Valorisez le champ **vads_validation_mode** :
   - À 0 pour une validation automatique (le paiement sera automatiquement remis en banque).

- À 1 pour une validation manuelle (opération effectuée depuis le Back Office Expert).

Le mode de validation s'applique à toutes les échéances.

5. Valorisez le champ **vads_currency** avec le code de la devise souhaitée en utilisant le tableau des devises.

6. Ajoutez les champs recommandés pour augmenter les chances de frictionless lors du paiement.

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

Exemple de formulaire de paiement en plusieurs fois (montants et dates d'échéance fixes) :

```
<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="3000" />
<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="MULTI:first=1000;count=3;period=30"/>
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190629180150" />
<input type="hidden" name="vads_trans_id" value="1N015m" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value= "zrhUNkAciZSEl6mS4BbhV3qkYUBB9RYJQCdg1kU0ELU="/>
<input type="submit" name="payer" value="Payer" />
</form>
```

Exemple de formulaire de paiement en plusieurs fois (montants et dates d'échéance personnalisées) :

):

```
<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="3000" />
<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="" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_config" value="
MULTI_EXT:20140201=1000;20140301=1000;20140401=1000" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190629130025" />
<input type="hidden" name="vads_trans_id" value="130025" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="7Sds6Z+R1Q1axRsblpChyQh5OU3oCle5FOirD4V/Bzk="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

9.4. Créer une autorisation sans remise

Ce mode de paiement vérifie la validité des données de la carte de l'acheteur sans la débiter.

Si nécessaire, vous pouvez débiter la carte du montant souhaité en utilisant la fonction **Dupliquer** du **Back Office Expert** et en procédant à une validation manuelle.

1. Utilisez tous les champs du tableau pour construire votre formulaire de paiement.

Nom du champ	Description	Format	Valeur
vads_site_id	Identifiant de la boutique	n8	Ex : 12345678
vads_ctx_mode	Mode de communication avec la plateforme de paiement	enum	TEST ou PRODUCTION
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_trans_date	Date et heure du formulaire de paiement dans le fuseau horaire UTC.	n14	Respectez le format AAAAMMJJHHMMSS Ex : 20200101130025
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_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_page_action	Action à réaliser	enum	PAYMENT
vads_version	Version du protocole d'échange avec la plateforme de paiement	enum	**V2**
vads_payment_config	Type de paiement	enum	SINGLE
vads_capture_delay	Délai avant remise en banque.	n..3	
vads_validation_mode	Mode de validation	n1	**1** (Manuelle)
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. Valorisez le champ **vads_amount** avec un montant faible, sans impact sur le plafond d'autorisation de carte.

3. Valorisez le champ **vads_validation_mode** à **1**.

4. Valorisez le champ **vads_currency** avec le code de la devise souhaitée en utilisant le tableau des devises.

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

Exemple de formulaire pour une autorisation sans remise :

```
<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="100" />
<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_page_action" value="PAYMENT" />
<input type="hidden" name="vads_validation_mode" value="1"/>
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190628073753" />
<input type="hidden" name="vads_trans_id" value="3jj7A8" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value= "DvltInRYXRroOZ/KnNdJSlpVr++29ZGty4nj1Y7yczU="/>
<input type="submit" name="payer" value="Payer" />
</form>
```

10. UTILISER DES FONCTIONS COMPLÉMENTAIRES

10.1. Gérer le retour vers le site marchand

A la fin du paiement, le navigateur de l'acheteur peut être redirigé vers une URL définie par le marchand. Cette URL est appelée **URL de retour**.

A ne pas confondre avec l'**URL de notification instantanée (également appelée IPN)** (voir chapitre **Gérer le dialogue vers le site marchand**).

10.1.1. Définir les URL de retour

Dans le formulaire de paiement, le marchand peut surcharger la configuration du Back Office Expert. Pour cela il peut:

- Utiliser 4 URL différentes en fonction du résultat du paiement:
  - Paiement accepté
  - Paiement refusé
  - Paiement abandonné
  - Paiement en erreur
- Utiliser une seule URL quel que soit le résultat du paiement.

10.1.1.1. Définir les URL de retour en fonction du résultat du paiement

Utilisez les champs facultatifs présentés dans le tableau ci-dessous pour concevoir le formulaire de paiement adapté à vos besoins.

Si aucune URL n'est valorisée dans le formulaire, la valeur configurée dans le Back Office Expert sera prise en compte.

Nom du champ	Description	Format	Valeur
vads_url_cancel	URL où sera redirigé l'acheteur après appui sur "annuler et retourner à la boutique" avant d'avoir procédé au paiement	ans..1024	Ex : http://demo.com/cancel.php
vads_url_error	URL où sera redirigé l'acheteur en cas d'erreur de traitement par la plateforme de paiement	ans..1024	Ex : http://demo.com/error.php
vads_url_refused	URL où sera redirigé l'acheteur, en cas de refus du paiement, après appui sur "retourner à la boutique"	ans..1024	Ex : http://demo.com/refused.php
vads_url_success	URL où sera redirigé l'acheteur, en cas de succès du paiement, après appui sur "retourner à la boutique"	ans..1024	Ex : http://demo.com/success.php

Exemple de formulaire de paiement avec définition d'URL de retour en fonction du résultat du 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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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="20191126101407" />
<input type="hidden" name="vads_trans_id" value="pm197W" />
<input type="hidden" name="vads_url_cancel" value="http://demo.com/cancel.php" />
<input type="hidden" name="vads_url_error" value="http://demo.com/error.php" />
<input type="hidden" name="vads_url_refused" value="http://demo.com/refused.php" />
<input type="hidden" name="vads_url_success" value="http://demo.com/success.php" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="lZIHzigiwCc6+uLStp8I5DQnbSqXu63Jtfo6Saeq3Mc="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

10.1.1.2. Définir une URL de retour unique quelque soit le résultat du paiement

Utilisez le champ facultatif **vads_url_return** pour définir l'url de redirection à la fin du paiement.

Si aucune URL n'est valorisée dans le formulaire, la valeur configurée dans le Back Office Expert sera prise en compte.

Exemple de formulaire de paiement avec une URL de retour unique quelque soit le résultat du 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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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="20191126101407" />
<input type="hidden" name="vads_trans_id" value="xrTYh2" />
<input type="hidden" name="vads_url_return" value="http://demo.com/return.php" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="ZI/GhI0GbeqqoXGeoZuPOy55SKQSYzRO1i6r5ku6vOs="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```


Tous droits réservés

10.1.2. Définir la méthode de réception des données

Pour des besoins de statistiques ou pour afficher des pages personnalisées, le site marchand doit pouvoir analyser certaines données transmises au navigateur de l'acheteur.

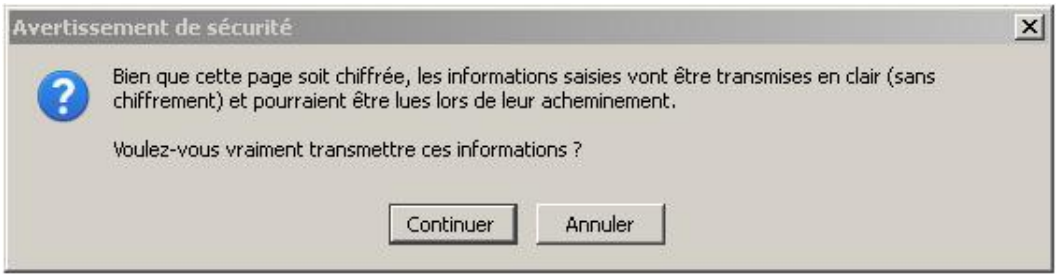
Par défaut, la plateforme de paiement ne transmet aucune donnée lors de la redirection vers l'URL de retour.

Le site marchand peut cependant activer l'envoi des données à l'URL de retour via le formulaire de paiement.

Utilisez le champ facultatif **vads_return_mode** pour indiquer la méthode de transmission des données vers le site marchand.

Valeur	Description
Absent, vide ou **NONE**	Aucune donnée n'est transmise.
GET	Les données sont transmises dans l'URL du navigateur.
POST	Les données sont transmises par formulaire HTTP **POST**.

La méthode **GET** permet d'éviter l'affichage d'un message d'avertissement lorsque le retour se fait sur un environnement **non sécurisé (http).**



Exemple de formulaire de paiement avec définition du mode de transmission des données :

```
<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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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_return_mode" value="GET" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190626101407" />
<input type="hidden" name="vads_trans_id" value="239848" />
<input type="hidden" name="vads_url_return" value="http://demo.com/return.php" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="oTCT+7Oc+xttdGmcp9qa6/0pSSfNxoMtl8U1J1l+LtE="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

10.2. Activer le retour automatique vers le site marchand

Le marchand peut indiquer dans son formulaire s'il souhaite rediriger automatiquement le navigateur de l'acheteur vers le site marchand à la fin du paiement.

Si vous utilisez un code de tracking (Google Analytics™ ou autre) sur votre site, vous devez implémenter cette fonctionnalité.

1. Utilisez les champs facultatifs ci-dessous en fonction de vos besoins.

Nom du champ	Description
vads_redirect_success_timeout	Définit le délai d'attente avant redirection après un paiement réussi. Ce délai est exprimé en seconde et doit être compris entre 0 et 300 secondes.
vads_redirect_success_message	Définit le message d'attente avant la redirection après un paiement réussi.
vads_redirect_error_timeout	Définit le délai d'attente avant redirection après un paiement refusé. Ce délai est exprimé en seconde et doit être compris entre 0 et 300 secondes.
vads_redirect_error_message	Définit le message d'attente avant la redirection après un paiement refusé.

Si vous choisissez un timeout à zéro votre redirection s'effectuera de la manière suivante :

- *Pour un **paiement accepté**, l'acheteur sera redirigé vers **vads_url_success**.*
- *Pour un **paiement annulé**, l'acheteur sera redirigé vers **vads_url_cancel** si le paramètre est défini.*
  - *Si le paramètre n'est pas renseigné, l'acheteur sera redirigé vers l'URL de retour renseignée dans le champ **vads_url_return** ou vers l'URL de retour renseignée dans le Back Office Expert.*
  - *Si l'URL de retour n'est pas définie, il sera redirigé vers l'URL de la boutique.*
- *Pour un **paiement refusé**, l'acheteur sera redirigé vers **vads_url_refused** si le paramètre est défini.*

2. Valorisez le champ **vads_return_mode** à **GET**.

Exemple de formulaire 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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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_redirect_error_message" value="Vous allez être redirigé vers
 votre site marchand" />
<input type="hidden" name="vads_redirect_error_timeout" value="0" />
<input type="hidden" name="vads_redirect_success_message" value="Vous allez être redirigé vers
 votre site marchand" />
<input type="hidden" name="vads_redirect_success_timeout" value="0" />
<input type="hidden" name="vads_return_mode" value="GET" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190626101407" />
<input type="hidden" name="vads_trans_id" value="AL3d8Q" />
<input type="hidden" name="vads_url_return" value="http://demo.com/return.php" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="AzTJmizS5N0muYzu63nVvCUWo0ixnMJfpqQmuEa4CSY="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

10.3. Définir le mode de remise en banque (automatique / manuel)

Le marchand peut paramétrer dans le Back Office Expert la manière dont sont envoyés les paiements à la banque (Menu **Paramétrage** > **Boutique** > onglet **Configuration**) :

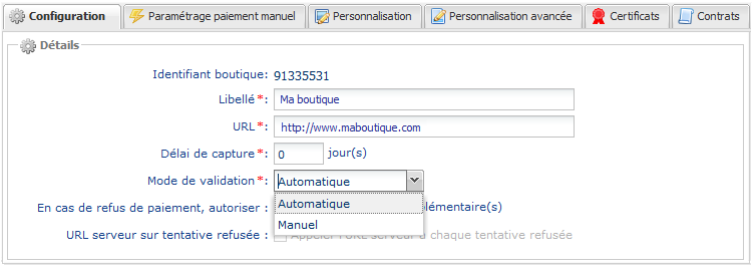


Image 8 : Définir le mode de remise en banque

- **Automatique** : aucune action nécessaire, les paiements sont remis en banque une fois le délai de remise atteint.
- **Manuel** : le marchand doit impérativement valider chaque paiement depuis son Back Office Expert ou par Web Services, pour qu'il soit remis en banque, et ceci, avant la date d'expiration de la demande d'autorisation.

  Toute transaction qui n'a pas été validée dans les délais impartis est considérée comme expirée et ne sera jamais remise en banque.

  Par défaut, le Back Office Expert est configuré pour remettre automatiquement en banque tous les paiements.

  Le marchand peut surcharger cette configuration dans son formulaire de paiement.

  Il devra implémenter les critères de son choix (état du stock, délai de réapprovisionnement, etc.) permettant de décider si la transaction doit être remise en banque automatiquement ou non.

  Utilisez le champ **vads_validation_mode** pour configurer le mode de remise en banque de la transaction (manuel ou automatique).

  Ce champ sera renvoyé dans la réponse avec la valeur transmise dans le formulaire.

Valeur	Description
Absent ou vide	Prend la valeur définie dans le Back Office Expert.
0	Remise en banque automatique. La transaction est validée automatiquement par la plateforme de paiement.
1	Remise en banque manuelle. La transaction doit être validée manuellement par le marchand depuis son Back Office Expert (ou automatiquement via l'utilisation de la fonction Web Service **Transaction/Validate**).

Exemple de formulaire de paiement avec définition du mode de remise en banque en mode INTERACTIVE :

```
<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="4000" />
<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_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="20190626164147" />
<input type="hidden" name="vads_trans_id" value="164147" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="vads_validation_mode" value="1" />
<input type="hidden" name="signature" value="cJFhNTLXQ4o6BgbW1pMMoM2yMilw90OIqmFjJ6DeUmA= />
<input type="submit" name="payer" value="Payer"/>
</form>
```


Tous droits réservés

10.4. Transmettre les données de l'acheteur

Les informations de l'acheteur (adresse e-mail, civilité, numéro de téléphone, etc.) constituent les informations de facturation.

Toutes les données transmises sont affichées dans le détail de la transaction (onglet **Client**) dans le Back Office Marchand.

Utilisez les champs facultatifs ci-dessous en fonction de vos besoins. *Ces champs seront renvoyés dans la réponse avec la valeur transmise dans le formulaire.*

Nom du champ	Description	Format	Valeur
vads_cust_email	Adresse e-mail de l'acheteur	ans..150	Ex : abc@example.com
vads_cust_id	Référence de l'acheteur sur le site marchand	an..63	Ex : C2383333540
vads_cust_national_id	Identifiant national	ans..255	Ex : 940992310285
vads_cust_title	Civilité de l'acheteur	an..63	Ex : M
vads_cust_status	Statut	enum	PRIVATE : pour un particulier **COMPANY** : pour une entreprise
vads_cust_first_name	Prénom	ans..63	Ex : Laurent
vads_cust_last_name	Nom	ans..63	Ex : Durant
vads_cust_legal_name	Raison sociale de l'acheteur	ans..100	Ex : D. & Cie
vads_cust_phone	Numéro de téléphone	an..32	Ex : 0467330222
vads_cust_cell_phone	Numéro de téléphone mobile	an..32	Ex : 06 12 34 56 78
vads_cust_address_number	Numéro de voie	ans..64	Ex : 109
vads_cust_address	Adresse postale	ans..255	Ex : Rue de l'innovation
vads_cust_address2	Deuxième ligne d'adresse	ans..255	Ex :
vads_cust_district	Quartier	ans..127	Ex : Centre ville
vads_cust_zip	Code postal	an..64	Ex : 31670
vads_cust_city	Ville	an..128	Ex : Labège
vads_cust_state	État / Région	ans..127	Ex : Occitanie
vads_cust_country	Code pays suivant la norme ISO 3166 alpha-2	a2	Ex : "FR" pour la France, "PF" pour la Polynésie Française, "NC" pour la Nouvelle Calédonie, "US" pour les Etats-Unis.

Exemple de formulaire de paiement avec informations sur l'acheteur

```
<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="4000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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="dupont.albert@exemple.com" />
<input type="hidden" name="vads_cust_first_name" value="Albert" />
<input type="hidden" name="vads_cust_last_name" value="Dupont" />
<input type="hidden" name="vads_cust_title" value="M." />
<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="20190627133115" />
<input type="hidden" name="vads_trans_id" value="522754" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="rEFhNTLXQ4o6BgbW1pTMoM2yMilw90OIqmFjJ6DeCxP="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

10.5. Transmettre les données de livraison

Les données de livraison de l'acheteur sont l'adresse, la civilité, le numéro de téléphone, etc..

Ces données seront affichées dans le Back Office Marchand en consultant le détail de la transaction (onglet **Client**).

Utilisez les champs facultatifs ci-dessous en fonction de vos besoins.

Ces champs seront renvoyés dans la réponse avec la valeur transmise dans le formulaire.

Nom du champ	Description	Format	Valeur
vads_ship_to_city	Ville	an..128	Ex : Bordeaux
vads_ship_to_country	Code pays suivant la norme ISO 3166 (obligatoire pour déclencher une ou plusieurs actions si le profil **Contrôle du pays de la livraison** est activé).	a2	Ex : FR
vads_ship_to_district	Quartier	ans..127	Ex : La Bastide
vads_ship_to_first_name	Prénom	ans..63	Ex : Albert
vads_ship_to_last_name	Nom	ans..63	Ex : Durant
vads_ship_to_legal_name	Raison sociale	an..100	Ex : D. & Cie
vads_ship_to_phone_num	Numéro de téléphone	ans..32	Ex : 0460030288
vads_ship_to_state	État / Région	ans..127	Ex : Nouvelle aquitaine
vads_ship_to_status	Définit le type d'adresse de livraison	enum	**PRIVATE** : pour une livraison chez un particulier **COMPANY** : pour une livraison en entreprise
vads_ship_to_street_number	Numéro de voie	ans..64	Ex : 2
vads_ship_to_street	Adresse postale	ans..255	Ex : Rue Sainte Catherine
vads_ship_to_street2	Deuxième ligne d'adresse	ans..255	
vads_ship_to_zip	Code postal	an..64	Ex : 33000

Exemple de formulaire de paiement avec informations sur la livraison

```
<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="4000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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_ship_to_city" value="la ville de livraison" />
<input type="hidden" name="vads_ship_to_country" value="FR" />
<input type="hidden" name="vads_ship_to_name" value="le nom du lieu de livraison" />
<input type="hidden" name="vads_ship_to_street" value="la rue pour effectuer la livraison" />
<input type="hidden" name="vads_ship_to_street_number" value="10" />
<input type="hidden" name="vads_ship_to_zip" value="31670" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190627143509" />
<input type="hidden" name="vads_trans_id" value="561095" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="bOIxHAgm4vYUq3oIDCdEPKOWgrB9bHzkfDBEAr1i10A="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

10.6. Transmettre les données de la commande

Le marchand peut indiquer dans son formulaire de paiement s'il souhaite transmettre les informations de la commande (numéro de la commande, description, contenu du panier etc.).

1. Utilisez les champs facultatifs ci-dessous en fonction de vos besoins.

Nom du champ	Description	Format	Valeur
vads_order_id	Numéro de commande Peut être composé de majuscules ou de minuscules, chiffres ou tiret ([A-Z] [a-z], 0-9, _, -).	ans..64	Ex : 2-XQ001
vads_order_info	Informations supplémentaires sur la commande	ans..255	Ex : Code interphone 3125
vads_order_info2	Informations supplémentaires sur la commande	ans..255	Ex : Sans ascenseur
vads_order_info3	Informations supplémentaires sur la commande	ans..255	Ex : Express
vads_nb_products	Nombre d'articles présents dans le panier	n..12	Ex : 2
vads_product_ext_idN	Code barre du produit dans le site web du marchand. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second et ainsi de suite).	an..100	Ex : vads_product_ext_id0 = "0123654789123654789" vads_product_ext_id1 = "0223654789123654789" vads_product_ext_id2 = "0323654789123654789"
vads_product_labelN	Libellé de l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second et ainsi de suite).	ans..255	Ex : vads_product_label0 = "tee-shirt" vads_product_label1 = "Biscuit" vads_product_label2 = "Sandwich"
vads_product_amountN	Prix TTC de l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second et ainsi de suite).	n..12	Ex : vads_product_amount0 = "1200" vads_product_amount1 = "800" vads_product_amount2 = "950"
vads_product_typeN	Type de l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second et ainsi de suite).	enum	Ex : vads_product_type0 = "CLOTHING_AND_ACCESSORIES" vads_product_type1 = "FOOD_AND_GROCERY" vads_product_type2 = "FOOD_AND_GROCERY"
vads_product_refN	Référence de l'article. N correspond à l'indice de l'article (0 pour le premier,	an..64	Ex : vads_product_ref0 = "CAA-25-006"

Tous droits réservés

Nom du champ	Description	Format	Valeur
	1 pour le second et ainsi de suite).		vads_product_ref1 = "FAG-B5-112" vads_product_ref2 = "FAG-S9-650"
vads_product_qtyN	Quantité d'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second et ainsi de suite).	n..12	Ex : vads_product_qty0 = "1" vads_product_qty1 = "2" vads_product_qty2 = "2"
vads_product_vatN	Montant ou taux de la TVA appliqué sur l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second et ainsi de suite). *La décimale est obligatoire pour exprimer un taux.* *La décimale est marquée par le caractère "."*.	n..12	• Valorisé avec un entier, sans décimale, pour exprimer un montant. Ex : 4525 pour 45,25 EUR • Valorisé avec un nombre décimal inférieur à 100, pour exprimer un taux. Ex : 20.0 ou 19.6532

2. Valorisez le champ vads_nb_products avec le nombre d'articles contenu dans le panier.

   Nous recommandons de rendre obligatoire la valorisation du champ pour prendre en compte le panier. Cela implique la valorisation des autres champs commençant par vads_product_ pour avoir les détails du panier.

3. Valorisez le champ **vads_product_amountN** avec le montant des différents articles contenus dans le panier dans l'unité la plus petite de la devise.

   N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).

4. Valorisez le champ **vads_product_typeN** avec la valeur correspondant au type de l'article.

   N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).

Valeur	Description
FOOD_AND_GROCERY	Produits alimentaires et d'épicerie
AUTOMOTIVE	Automobile / Moto
ENTERTAINMENT	Divertissement / Culture
HOME_AND_GARDEN	Maison / Jardin
HOME_APPLIANCE	Equipement de la maison
AUCTION_AND_GROUP_BUYING	Ventes aux enchères / Achats groupés
FLOWERS_AND_GIFTS	Fleurs / Cadeaux
COMPUTER_AND_SOFTWARE	Ordinateurs / Logiciels
HEALTH_AND_BEAUTY	Santé / Beauté
SERVICE_FOR_INDIVIDUAL	Services à la personne
SERVICE_FOR_BUSINESS	Services aux entreprises
SPORTS	Sports
CLOTHING_AND_ACCESSORIES	Vêtements / Accessoires

Valeur	Description
TRAVEL	Voyage
HOME_AUDIO_PHOTO_VIDEO	Son / Image / Vidéo
TELEPHONY	Téléphonie

5. Valorisez le champ **vads_product_labelN** avec le libellé de chacun des articles contenus dans le panier.
   N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).

6. Valorisez le champ **vads_product_qtyN** avec la quantité de chacun des articles contenus dans le panier.
   N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).

7. Valorisez le champ **vads_product_refN** avec la référence de chacun des articles contenus dans le panier.
   N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).

8. Contrôlez la valeur du champ **vads_amount**. Elle doit correspondre au montant total de la commande.

Exemple de formulaire de paiement avec description du panier "vads_product_xxx" :

```
<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="11000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_nb_products" value="2"/>
<input type="hidden" name="vads_product_amount0" value="5000" />
<input type="hidden" name="vads_product_label0" value="produit1" />
<input type="hidden" name="vads_product_qty0" value="2" />
<input type="hidden" name="vads_product_ref0" value="ref1" />
<input type="hidden" name="vads_product_amount1" value="1000" />
<input type="hidden" name="vads_product_label1" value="produit2" />
<input type="hidden" name="vads_product_qty1" value="1" />
<input type="hidden" name="vads_product_ref1" value="ref2" />
<input type="hidden" name="vads_order_id" value="CD100000857" />
<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="20190627145218" />
<input type="hidden" name="vads_trans_id" value="571381" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="xYw1UnU3BACGhf3UEyqbQzpwuvZDEkCAWAE5fgbtfxI="/>
<input type="submit" name="payer" value="Payer"/></form>
```

10.7. Transmettre la préférence 3-D Secure

Utilisez le champ **vads_threeds_mpi** pour transmettre votre préférence:

Cas d'utilisation	Valeurs	Description
CHALLENGE : avec interaction du porteur	**1**	**Déprécié**.
	3	**Challenge Requested (3DS Requestor Preference)** : permet de demander une authentification forte pour la transaction.
	4	**Challenge Requested (Mandate)** :permet d'indiquer que pour des raisons réglementaires, une authentification forte est requise pour la transaction.
FRICTIONLESS : sans interaction du porteur	**2***	Permet de demander une exemption à l'authentification forte : • Transactions à faible montant. • Transaction Risk Analysis (TRA Acquéreur). • Safe'R by CB. Plus d'infos : Tableau des exemptions, ci-après.
	6	**No Challenge Requested (Data share only)** : Transaction sans interaction du porteur (ni authentification) mais le marchand souhaite partager les données via le processus 3DS avec l'émetteur pour réduire le risque de refus lors de l'autorisation. Utilisé en Amérique Latine.
Pas de préférence 3-D Secure	**0 ou absent ou vide**	Le choix de la préférence est délégué à l'émetteur de la carte. Si l'émetteur décide de réaliser une authentification sans interaction (frictionless), le paiement sera garanti.
	5	

* **Tableau des exemptions** :

Exemptions	Description
Transactions à faible montant	En Europe, vous pouvez demander une exemption à l'authentification forte, pour les transactions d'un montant inférieur à 30 EUR, et dans la limite soit de 5 opérations successives ou d'un montant cumulé inférieur à 100 EUR. Si le montant est supérieur à 30 EUR, la valeur transmise par le marchand est ignorée et le choix de la préférence est délégué à l'émetteur de la carte (No Preference). Pour les paiements réalisés dans une devise différente de l'euro, une demande de frictionless est transmise à l'émetteur. Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte. Si la boutique ne dispose pas de l'option "Frictionless 3DS2", le choix de la préférence est délégué à l'émetteur de la carte (No Preference).
Transaction Risk Analysis (TRA Acquéreur)	Si votre boutique dispose de l'option "TRA Acquéreur 3DS2", vous pouvez demander à l'émetteur une exemption à l'authentification forte lorsque le montant est inférieur au seuil fixé par votre établissement financier. Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.

Tous droits réservés

Exemptions	Description
	L'activation de l'option "TRA Acquéreur 3DS2" est soumise à l'accord préalable de votre établissement financier.

Safe'R by CB	CB propose le programme Safe'R by CB. Ce programme a pour objectif de répondre aux attentes des marchands à très faible risque et au volumétrie importante. Vous pouvez demander une exemption à l'authentification forte :
	• Si le montant est inférieur à 100 EUR, l'exemption est systématique pour les marchands éligibles.
	• Si le montant est compris entre 100 EUR et 250 EUR, une expérimentation est en cours. Pour en bénéficier, le marchand doit :
	  • Avoir un contrat CB.
	  • Être éligible à la TRA acquéreur.
	  • Transmettre les valeurs requises dans le flux 3-D Secure, selon les règles définies par la plateforme.
	Si la demande de frictionless est acceptée, la transaction ne bénéficie pas du transfert de responsabilité en cas de contestation du porteur de carte.
	Pour bénéficier du programme Safe'R by CB, vous devez contacter l'administration des ventes pour obtenir un accord explicite.

Tous droits réservés

10.8. Surcharger l'URL de notification instantanée (IPN)

Vous pouvez surcharger l'URL de notification instantanée (également appelée IPN) dans le formulaire dans le cas où vous utilisez une seule boutique pour différents canaux de ventes, différentes typologies de paiement, différentes langues etc…

Cette fonctionnalité est incompatible avec l'exécution, depuis le Back Office Expert, de la requête envoyée à l'URL de notification instantanée. L'URL appelée sera celle configurée dans la règle de notification (voir chapitre **Paramétrer les notifications**).

Utilisez le champ **vads_url_check** pour surcharger l'URL de la page à notifier.

Si la valeur du champ **vads_url_check** est erronée, le formulaire sera rejeté.

Exemple de formulaire de paiement qui surcharge l'URL de notification instantanée:

```
<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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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="20190626101407" />
<input type="hidden" name="vads_trans_id" value="239848" />
<input type="hidden" name="vads_url_check" value="http://www.myshop.com/check" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="yXvSZnYvcMRORVGiapWaHT0euKDI0OGlrddYKc4XDZc="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

10.9. Définir le contrat commerçant

Le marchand peut spécifier dans son formulaire de paiement la valeur du contrat commerçant à utiliser.

Cette fonctionnalité n'est utile que si vous possédez plusieurs contrats acceptant la même devise sur un même réseau d'acceptation.

Utilisez le champ facultatif **vads_contracts** pour définir le contrat commerçant à utiliser.

- Pour **définir une liste** de contrats, séparez les valeurs par un point-virgule « ; »

```
vads_contracts=CODE_RESEAU_A=MID_A1;CODE_RESEAU_B=MID_B2
```

- Pour **exclure un réseau**, ajoutez **nom du réseau**=**NO**.

```
vads_contracts=CODE_RESEAU_A=NO
```

- Pour **forcer le TID**, séparez le numéro de contrat et le numéro de TID par un deux-points: « : »

```
vads_contracts=CODE_RESEAU_A=MID_A1:TID_1
```

- Si le champ est envoyé à vide, le contrat utilisé sera celui défini par l'ordre de priorité dans le Back Office Expert (Menu **Paramétrage** > **Boutique** > onglet **Association contrats**).

Liste des réseaux disponibles:

Code Réseau	Description
ACCORD_SANDBOX	Réseau Oney (cartes cadeau et privatives) - mode sandbox
ACCORD	Réseau Oney (cartes cadeau et privatives)
ALIPAY_PLUS	Réseau Alipay+
ALMA	Réseau ALMA
AMEXGLOBAL	Réseau American Express
AURORE	Réseau CETELEM Aurore (cartes Enseignes et cartes Aurore Universelles)
BIZUM	Réseau Bizum Bancário
CB	Réseau CB
CONECS	Réseau Titre-Restaurant Conecs
COFIDIS	Réseau Cofidis
CVCONNECT	Réseau Chèque-Vacances Connect
DFS	Réseau DFS (Discover Financial Services)
EDENRED	Réseau Edenred (Tickets Restaurant, Tickets EcoChèque, Tickets Compliments, Ticket Chèque Consommation)
FLOA	Réseau Floa
FRANFINANCE	Réseau Franfinance
FRANFINANCE_SB	Réseau Franfinance - mode sandbox)
FULLCB	Réseau FULL CB (Paiement en 3 ou 4 fois sans frais par BNPP PF)
GATECONEX	Réseau GATECONEX

Code Réseau	Description
GICC_DINERS	Réseau GICC (cartes Diners Club)
GICC_MAESTRO	Réseau GICC (cartes Maestro)
GICC_MASTERCARD	Réseau GICC (cartes Mastercard)
GICC_VISA	Réseau GICC (cartes Visa)
GICC	Réseau GICC
ILLICADO	Réseau Illicado
IP	Réseau Initiation de paiement (Virement SEPA et Virement SEPA Instantané)
JCB	Réseau JCB
LYRA_COLLECT_PPRO	Réseau PPRO
MULTIBANCO	Réseau MULTIBANCO
NPCIUPI	Réseau UPI
ONEY_API	Réseau Oney API
ONEY_API_SB	Réseau Oney API - mode sandbox
ONEY_SANDBOX	Réseau Oney (Paiement en 3 ou 4 fois par FacilyPay) - mode sandbox
ONEY	Réseau Oney (Paiement en 3 ou 4 fois par FacilyPay)
PAYCONIQ	Réseau payconiq
PAYDIREKT_V2	Réseau PayDirekt V2
PAYPAL	Réseau PayPal
PAYPAL_SB	Réseau PayPal - mode sandbox
PLANET_DCC	Réseau Planet
POSTFINANCEV2	Réseau POSTFINANCE
REDSYS_REST	Réseau RedSys REST
SEPA	Réseau SEPA (SDD et SCT)
WECHAT_PAY	Réseau WeChat Pay

Exemples:

Vous disposez de:

- deux contrats sur le réseau A: MID_A1 et MID_A2
- deux contrats sur le réseau B: MID_B1 et MID_B2

Pour spécifier le contrat à utiliser pour ces deux réseaux, **vads_contracts** devra être valorisé de la manière suivante:

```
vads_contracts=A=MID_A2;B=MID_B1
```

Pour proposer un paiement uniquement sur le contrat MID_A1 et empêcher les paiements sur le réseau B, valorisez **vads_contracts** comme suit:

```
vads_contracts=A=MID_A1;B=NO
```

Pour forcer le TID à utiliser sur le réseau A:

```
vads_contracts=A=MID_A1:TID_A1
```


Tous droits réservés

10.10. Créer des champs spécifiques en fonction de vos besoins

Le marchand peut transmettre des informations spécifiques dans le formulaire de paiement. Il peut par exemple ajouter une information complémentaire dans l'e-mail de confirmation de paiement qu'il recevra.

Cette information sera visible dans le Back Office, dans le détail de la transaction (onglet **Extras**), et sera également retournée dans l'URL de notification.

Le nom doit commencer par **vads_ext_info** pour être pris en compte.

vads_ext_info_*lenomduchamp*=valeur

1. Utilisez l'ensemble des champs nécessaires à votre cas d'utilisation (voir chapitre "Générer un formulaire de paiement") pour construire votre formulaire de paiement.

2. Utilisez le champ facultatif **vads_ext_info** en fonction de vos besoins en respectant la syntaxe :

   vads_ext_info_*lenomduchamp*=*valeur*

   Où :

   - ***lenomduchamp***

     Permet de définir le nom du champ.

   - ***valeur***

     Permet de définir la valeur du champ.

   Il n'a pas de restriction sur le nombre de champs spécifiques créés.

   Ce ou ces champs seront renvoyés dans la réponse avec la valeur transmise dans le formulaire.

3. 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").

```
<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="4000" />
<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_ext_info_qty_articles" value="2" /> />
[...]
<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="20150826133115" />
<input type="hidden" name="vads_trans_id" value="722754" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="7896adcaf7338930db9715afa123531f42"/>
<input type="submit" name="payer" value="Payer"/>
</form>
```


Tous droits réservés

10.11. Transmettre les données du sous-marchand

Le facilitateur de paiement peut transmettre les données du sous-marchand concerné par la transaction.

Nom du champ	Description	Format
vads_submerchant_address	Adresse du sous-marchand. Transmis par le facilitateur de paiement.	ans..255
vads_submerchant_address2	Complément de l'adresse du sous-marchand. Transmis par le facilitateur de paiement.	ans..255
vads_submerchant_city	Ville du sous-marchand. Transmis par le facilitateur de paiement.	ans..128
vads_submerchant_company_type	Type de société du sous-marchand. Transmis par le facilitateur de paiement.	ans..60
vads_submerchant_country	Pays de l'adresse du sous-marchand (norme ISO 3166 alpha-2). Transmis par le facilitateur de paiement.	a2
vads_submerchant_facilitatorId	Identifiant du facilitateur de paiement.Transmis par le facilitateur de paiement.	ans..128
vads_submerchant_legal_number	Numéro légal du sous-marchand. Transmis par le facilitateur de paiement.	ans..24
vads_submerchant_mcc	Code MCC du sous-marchand. Transmis par le facilitateur de paiement.	n4
vads_submerchant_mid	Numéro de contrat (MID) du sous-marchand. Transmis par le facilitateur de paiement.	n..64
vads_submerchant_name	Raison sociale du sous-marchand. Transmis par le facilitateur de paiement.	ans..255
vads_submerchant_phone	Numéro de téléphone du sous-marchand. Transmis par le facilitateur de paiement.	ans..32
vads_submerchant_soft_descriptor	Libellé (soft-descriptor) du sous-marchand qui apparaît sur le relevé d'opérations bancaires de l'acheteur. Transmis par le facilitateur de paiement.	ans..255
vads_submerchant_state	Région de l'adresse du sous-marchand. Transmis par le facilitateur de paiement.	ans..128
vads_submerchant_url	URL du sous-marchand. Transmis par le facilitateur de paiement.	ans..128
vads_submerchant_zip	Code postal du sous-marchand. Transmis par le facilitateur de paiement.	an..64

10.12. Transmettre les données à un ou plusieurs réseaux

Le marchand peut transmettre des informations spécifiques à un ou plusieurs réseaux.

Utilisez le champ **vads_acquirer_transient_data** en fonction de vos besoins. Voir : Dictionnaire de données

Exemple

Tous droits réservés

Pour limiter les cartes acceptées pour le paiement en fonction du code BIN, le format attendu est le suivant :

```
vads_acquirer_transient_data={"MULTI":{"bins":["bin1","bin2","bin3"]}}
```

NB: Supporte les codes BIN à 6 chiffres ou les codes BIN à 8 chiffres.

- code BIN à **6 chiffres**: 4012 34XX XXXX XXXX
- code BIN à **8 chiffres**: 4000 1234 XXXX XXXX

Exemple de formulaire 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_acquirer_transient_data" value="{"MULTI":{"bins":
["401234","40001234"]}}" />
<input type="hidden" name="vads_amount" value="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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="20190626101407" />
<input type="hidden" name="vads_trans_id" value="AL3d8Q" />
<input type="hidden" name="vads_url_return" value="http://demo.com/return.php" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="AzTJmizS5N0muYzu63nVvCUWo0ixnMJfpqQmuEa4CSY="/>
input type="submit" name="payer" value="Payer"/>
</form>
```

11. PERSONNALISER LES PAGES DE PAIEMENT

Vous pouvez personnaliser certains éléments de la page de paiement :

- les moyens de paiement proposés au moment du paiement,
- la langue dans laquelle seront affichées les pages de paiement,
- les langues proposées à l'acheteur sur les pages de paiement,
- le nom et l'URL de la boutique,
- le libellé des boutons.

Grâce à l'option de **personnalisation avancée**, vous pouvez aussi:

- créer différents modèles de personnalisation de la page de paiement afin de la rendre visuellement proche de votre site marchand.
- créer différents modèles de personnalisation des e-mails à destination de l'acheteur
- personnaliser certains libellés apparaissant sur les pages de paiement.

Ceci aura pour effet de rassurer l'acheteur lors de la redirection pour procéder au paiement.

Consultez le manuel utilisateur Personnalisation avancée pour plus de détails ou contactez l'administration des ventes.

11.1. Surcharger le modèle de personnalisation

Le Back Office Expert permet :

- de créer plusieurs modèles de personnalisation des pages de paiement,
- de définir le modèle qui s'appliquera par défaut pour toutes vos transactions.

Le formulaire de paiement permet de surcharger dynamiquement le modèle à appliquer grâce au champ **vads_theme_config**.

Pour cela, vous devez utiliser le mot-clé : **RESPONSIVE_MODEL** et indiquer le nom du modèle à appliquer (Model_1, Model_2, ...).

Exemple d'utilisation:

```
<input type="hidden" name="vads_theme_config" value="RESPONSIVE_MODEL=Model_1" />
```

Consultez le *Manuel d'utilisation du Back Office - Personnalisation avancée* pour plus de détails sur la création des modèles.

Consultez la description du champ vads_theme_config pour plus de détails sur l'utilisation de ce champ.

11.2. Gérer les moyens de paiement proposés à l'acheteur

Il est possible de personnaliser les moyens de paiement proposés à l'acheteur en utilisant le champ **vads_payment_cards**.

Il est recommandé de proposer sur le site marchand un bouton de paiement différent pour chaque moyen de paiement et de transmettre le choix de l'acheteur dans **vads_payment_cards**.

La liste des valeurs possibles est décrite dans le Dictionnaire de données.

Pour plus d'informations, consultez la documentation dédiée à chaque moyen de paiement que vous souhaitez proposer .

Pour proposer le paiement par carte CB, Visa, Mastercard, Maestro, Visa Electron et e-CB, nous vous suggérons d'envoyer uniquement la valeur **CB**.

Pour proposer le paiement par carte via des acquéreurs européens (Elavon, Six, Concardis, VR Pay etc...), nous vous suggérons d'envoyer la valeur "**VISA**" ou "**MASTERCARD**".

Ainsi l'acheteur est redirigé sur la page de saisie des données cartes, et le type de carte est automatiquement détecté.

Il est vivement déconseillé de laisser le champ vide. En cas d'ajout de nouveau moyen de paiement sur votre boutique, il serait proposé automatiquement, même si vous ne souhaitez pas le proposer.

Exemple de formulaire de paiement avec liste de choix de moyens 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="30000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_cards" value="CB" />
<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="20190626101407" />
<input type="hidden" name="vads_trans_id" value="239848" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="qqpxF6z1+Ri5jtkHNVDCCJulxxpJYehrfP1OLwJ4Ysg="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

11.3. Modifier la langue

Vous pouvez personnaliser la langue utilisée sur les pages de paiement.

Valorisez le champ **vads_language** avec une des valeurs présentes dans le tableau ci-dessous.

Langue	Codification ISO 639-1
Allemand	de
Anglais	en
Chinois	zh
Espagnol	es
Français	fr
Italien	it
Japonais	ja
Néerlandais	nl
Polonais	pl
Portugais	pt
Russe	ru
Suédois	sv
Turc	tr

- Si la valeur du champ **vads_language** est erronée, le formulaire sera rejeté.
- Si le champ n'est pas envoyé ou s'il est valorisé à vide, la page de paiement sera affichée dans la langue du navigateur de l'acheteur.
- L'acheteur pourra à tout moment changer de langue en utilisant le sélecteur de langue présent en haut à droite de la page de paiement.

Exemple de formulaire de paiement avec définition de la langue :

```
<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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_language" value="fr" />
<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="20190626101407" />
<input type="hidden" name="vads_trans_id" value="239848" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="PAMdHJ8FJc2CqUJLXQLxz+e77K4k1YGJmI5mHqGN74g="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

11.4. Modifier les langues proposées à l'acheteur

Vous pouvez personnaliser la liste des langues proposées à l'acheteur par le sélecteur de langues présent en haut à droite de la page de paiement.

La dernière langue sélectionnée par l'acheteur sera la langue par défaut de l'e-mail de confirmation de paiement à destination de l'acheteur.

Valorisez le champ **vads_available_languages** en utilisant le tableau ci-dessous :

- avec une seule valeur si vous ne souhaitez pas que l'acheteur change de langue.
- **avec une liste de valeurs séparées par un « ; »** pour lister les langues disponibles.

Langue	Valeur	Langue disponible par défaut
Allemand	de	x
Anglais	en	x
Chinois	zh	x
Espagnol	es	x
Français	fr	x
Italien	it	x
Japonais	ja	x
Néerlandais	nl	x
Polonais	pl	
Portugais	pt	x
Russe	ru	x
Suédois	sv	x
Turc	tr	

Si la valeur du champ **vads_available_languages** est erronée, le formulaire sera rejeté.

Exemple de formulaire de paiement avec liste de choix de langues :

```
<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="3000" />
<input type="hidden" name="vads_available_languages" value="fr;en;nl;de" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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="20190626101407" />
<input type="hidden" name="vads_trans_id" value="239848" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="aEWutqzuHH6Q8ns3a6cj5XitZCuhYsDcsKjlLpL8flA="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```


Tous droits réservés

11.5. Modifier le nom et l'URL de la boutique

Si vous possédez deux noms de domaines, vous pouvez modifier le nom et l'URL de la boutique pour faire apparaître le nom du domaine.

1. Utilisez le champ **vads_shop_name** pour afficher le nom de la boutique affiché sur le récapitulatif à la fin du paiement, le ticket et les e-mails de confirmation.

2. Utilisez le champ **vads_shop_url** pour modifier l'URL de la boutique affichée sur les pages de paiement.

   Cette valeur sera reprise dans l' e-mail de confirmation.

   Si la valeur du champ **vads_shop_url** est erronée, le formulaire ne sera pas rejeté.

Exemple de formulaire de paiement avec modification du nom et de l'URL de la boutique :

```
<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="3000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<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_shop_name" value="My Shop" />
<input type="hidden" name="vads_shop_url" value="http://www.myshop.com" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20190626101407" />
<input type="hidden" name="vads_trans_id" value="239848" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="gV0f2HZzQ9BxttHM2W5ZM+AKQsxu0HjDvKy0NAE/G24="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

11.6. Modifier le libellé du bouton « Retourner à la boutique »

Vous pouvez personnaliser le texte **« Retourner à la boutique »**.

1. Utilisez le champ **vads_theme_config** pour modifier le libellé des boutons « Retourner à la boutique ».

2. Utilisez le mot-clé **SUCCESS_FOOTER_MSG_RETURN** pour modifier le libellé du bouton « Retour à la boutique » affiché en cas de paiement accepté.

3. Utilisez le mot-clé **CANCEL_FOOTER_MSG_RETURN** pour modifier le libellé du bouton « Annuler et retourner à la boutique » affiché sur les différentes pages de paiement.

En souscrivant à l'option **personnalisation avancée**, vous pourrez modifier des libellés (exemple : identifiant du marchand) affichés sur la page de paiement.

Voir : Manuel d'utilisation du Back Office Personnalisation avancée pour plus de détails ou contactez l'administration des ventes.

Exemple de formulaire de paiement qui modifie le libellé du bouton « Retourner à la boutique » :

```
<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="4000" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="PRODUCTION" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_order_id" value="CD100000858" />
<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_theme_config"
 value="CANCEL_FOOTER_MSG_RETURN=Annuler;SUCCESS_FOOTER_MSG_RETURN=Retour" />
<input type="hidden" name="vads_trans_date" value="20190631092024" />
<input type="hidden" name="vads_trans_id" value="408248" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="ge5DHBbUGsq4cFfSIR1QyB/L/9qPNp2vhX9/G3kKJeQ="/>
<input type="submit" name="payer" value="Payer"/>
</form>
```

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`.

Tous droits réservés

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=

12.1. Exemple d'implémentation en JAVA

Définition d'une classe utilitaire Sha utilisant l'algorithme HMAC-SHA-256 pour calculer la signature :

```
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.io.UnsupportedEncodingException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.Base64;
import java.util.TreeMap;

public class VadsSignatureExample {
 /**
  * Build signature (HMAC SHA-256 version) from provided parameters and secret key.
  * Parameters are provided as a TreeMap (with sorted keys).
  */
 public static String buildSignature(TreeMap<String, String> formParameters, String
  secretKey) throws NoSuchAlgorithmException, InvalidKeyException, UnsupportedEncodingException
 {
   // Build message from parameters
   String message = String.join("+", formParameters.values());
   message += "+" + secretKey;
   // Sign
   return hmacSha256Base64(message, secretKey);
  }
    /**
    * Actual signing operation.
    */
 public static String hmacSha256Base64(String message, String secretKey) throws
  NoSuchAlgorithmException, InvalidKeyException, UnsupportedEncodingException {
   // Prepare hmac sha256 cipher algorithm with provided secretKey
   Mac hmacSha256;
   try {
    hmacSha256 = Mac.getInstance("HmacSHA256");
   } catch (NoSuchAlgorithmException nsae) {
    hmacSha256 = Mac.getInstance("HMAC-SHA-256");
   }
   SecretKeySpec secretKeySpec = new SecretKeySpec(secretKey.getBytes("UTF-8"), "HmacSHA256");
   hmacSha256.init(secretKeySpec);
   // Build and return signature
   return Base64.getEncoder().encodeToString(hmacSha256.doFinal(message.getBytes("UTF-8")));
  }
}
```

Définition d'une classe utilitaire Sha utilisant l'algorithme SHA-1 pour calculer la signature :

```
import java.security.MessageDigest;
import java.security.SecureRandom;

public class Sha {
    static public final String SEPARATOR = "+" ;
    public static String encode(String src) {
        try {
            MessageDigest md;
            md = MessageDigest.getInstance( "SHA-1" );
            byte bytes[] = src.getBytes( "UTF-8" );
            md.update(bytes, 0, bytes. length );
            byte[] sha1hash = md.digest();
            return convertToHex(sha1hash);
        }
        catch(Exception e){
            throw new RuntimeException(e);
        }
    }
    private static String convertToHex(byte[] sha1hash) {
        StringBuilder builder = new StringBuilder();
            for (int i = 0; i < sha1hash. length ; i++) {
               byte c = sha1hash[i];
               addHex(builder, (c >> 4) & 0xf);
               addHex(builder, c & 0xf);
        }
        return builder.toString();
    }
    private static void addHex(StringBuilder builder, int c) {
        if (c < 10)
            builder.append((char) (c + '0' ));
        else
            builder.append((char) (c + 'a' - 10));
    }
}
```


Tous droits réservés

Fonction qui calcule la signature :

```
public ActionForward performCheck(ActionMapping actionMapping, BasicForm form,
    HttpServletRequest request, HttpServletResponse response){
        SortedSet<String> vadsFields = new TreeSet<String>();
        Enumeration<String> paramNames = request.getParameterNames();

        // Recupere et trie les noms des champs vads_* par ordre alphabetique
        while (paramNames.hasMoreElements()) {
            String paramName = paramNames.nextElement();
            if (paramName.startsWith( "vads_" )) {
               vadsFields.add(paramName);
            }
        }
        // Calcule la signature
        String sep = Sha.SEPARATOR;
        StringBuilder sb = new StringBuilder();
        for (String vadsParamName : vadsFields) {
            String vadsParamValue = request.getParameter(vadsParamName);
            if (vadsParamValue != null) {
               sb.append(vadsParamValue);
            }
            sb.append(sep);
        }
        sb.append( shaKey );
        String c_sign = Sha.encode(sb.toString());
        return c_sign;
}
```

12.2. Exemple d'implémentation en PHP

Exemple de calcul de signature utilisant l'algorithme HMAC-SHA-256 :

```
function getSignature ($params,$key)
{
    /**
     *Function that computes the signature.
     * $params : table containing the fields to send in the payment form.
     * $key : TEST or PRODUCTION key
     */
    //Initialization of the variable that will contain the string to encrypt
    $signature_content = "";

    //sorting fields alphabetically
    ksort($params);
    foreach($params as $name=>$value){

        //Recovery of vads_ fields
        if (substr($name,0,5)=='vads_'){

            //Concatenation with "+"
            $signature_content .= $value."+";
         }
    }
    //Adding the key at the end
    $signature_content .= $key;

    //Encoding base64 encoded chain with SHA-256 algorithm
    $signature = base64_encode(hash_hmac('sha256',$signature_content, $key, true));
    return $signature;
 }
```

Exemple de calcul de signature utilisant l'algorithme SHA-1 :

```
function getSignature($params, $key)
{
    /**
     * Function that computes the signature.
     * $params : table containing the fields to send in the payment form.
     * $key : TEST or  PRODUCTION key
     */
    //Initialization of the variable that will contain the string to encrypt
    $signature_content = "" ;

    // Sorting fields alphabetically
    ksort($params);
        foreach ($params as $name =>$value)
    {
    // Recovery of vads_ fields
        if (substr($name,0,5)=='vads_') {
            // Concatenation with "+"
            $signature_content .= $value."+";
        }
    }
    // Adding the key at the end
    $signature_content .= $key;

    // Applying SHA-1 algorithm
    $signature = sha1($signature_content);
    return $signature ;
}
```


Tous droits réservés

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="1315" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_cust_id" value="1234" />
<input type="hidden" name="vads_cust_email" value="jg@sample.com" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_order_id" value="CMD012859" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_cards" value="VISA;MASTERCARD" />
<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="20200326101407" />
<input type="hidden" name="vads_trans_id" value="362812" />
<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 :

Tous droits réservés

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).

Tous droits réservés

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.

13.3. Gérer les timeout

Notion de session de paiement

Une "session de paiement" est le temps passé par un acheteur sur la page de paiement.

La session de paiement débute dès la reception du formulaire par la plateforme de paiement.

La durée de la session est de 10 minutes (sauf exception pour certains moyens de paiement).

Cette durée est :

- **suffisante** pour permettre à chaque acheteur de réaliser son paiement
- **fixe** : elle n'est pas remise à zéro à chaque action de l'utilisateur
- **non modifiable** : elle est fixée par la plateforme de paiement pour répondre à des contraintes techniques.

Passé ce délai, la session expire et les données de session sont purgées.

Expiration de la session de paiement

Il est possible que dans certains cas, la session de paiement expire alors que l'acheteur n'a pas terminé son paiement.

Cas les plus fréquents :

1. Une fois redirigé sur la page de paiement, l'acheteur se rend compte qu'il est temps pour lui d'aller déjeuner, par exemple.

   Une heure plus tard, il décide de continuer son paiement et clique sur le logo correspondant à son moyen de paiement.

   Sa session de paiement ayant expirée, la plateforme de paiement affiche un message d'erreur lui indiquant qu'il a été déconnecté suite à une trop longue inactivité.

   L'acheteur a alors la possibilité de cliquer sur un bouton pour retourner sur le site marchand.

   Le retour à la boutique se fait vers l'URL spécifiée par le marchand :

   - dans le champ *vads_url_return* transmis dans le formulaire de paiement,
   - dans le champ "URL de la boutique" du Back Office Expert, si l'URL n'est pas spécifiée dans le champ *vads_url_return* du formulaire de paiement.
2. Une fois redirigé sur la page de paiement, l'acheteur ferme son navigateur (par erreur ou parce qu'il ne souhaite plus procéder au paiement).

Notification en cas d'expiration de session

Le site marchand a la possibilité d'être notifié en cas d'expiration de session.

Pour cela le marchand doit configurer et activer la règle ***URL de notification sur annulation*** (voir chapitre Paramétrer les notifications).

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.

Tous droits réservés

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.

Pour un bon fonctionnement des notifications, suivez ces recommandations :

- 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.
- Evitez les redirections, car elles entraînent la perte des données présentes dans le POST, comme par exemple "https://**www.**example.com" vers "https://example.com" ou "**http**://example.com" vers "**https**://example.com".

  Vérifiez la configuration de vos équipements ou contactez votre hébergeur.
- Evitez le contenu HTML.

  L'accès aux ressources telles que les images ou feuilles de styles peuvent ralentir les échanges entre Lyra Collect et le site marchand.
- Testez votre URL sur le site de Qualys SSL Labs (https://www.ssllabs.com/ssltest/).

  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.
- 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 délai de traitement est important.

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.

- Assurez-vous que le temps de traitement de l'IPN soit le plus court possible. **Lyra Collect recommande 10 secondes maximum**. L' objectif est :
  - 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 système d'information afin que celui-ci soit conforme au résultat du paiement
- Au-delà de 35 secondes, Lyra Collect stoppe l'appel et déclenche un timeout.

Tous droits réservés

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.

Tous droits réservés

14.5. Analyser la nature de la notification

Lors d'une notification le champ **vads_url_check_src** permet de différencier les notifications en fonction de leur évènement déclencheur :

- création d'une transaction.
- 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, ...

14.6. Traiter les données de la réponse

Ci-dessous un exemple d'analyse pour vous guider pas à pas lors du traitement des données de la réponse.

Consultez le le dictionnaire de données pour obtenir la description et le format des champs.

1. Identifiez le mode (TEST ou PRODUCTION) dans lequel a été créé la transaction en analysant la valeur du champ **vads_ctx_mode.**

2. Identifiez la commande en récupérant la valeur du champ **vads_order_id** si vous l'avez transmis dans le formulaire de paiement.

   Vérifiez que le statut de la commande n'a pas déja été mis à jour.

3. Récupérez le résultat du paiement transmis dans le champ **vads_trans_status**.

   Sa valeur vous permet de définir le statut de la commande.

Valeur	Description
ABANDONED	**Abandonné** Paiement abandonné par l'acheteur. La transaction n'est pas créée et **n'est donc pas visible dans le Back Office Expert.**
ACCEPTED	**Accepté**. Statut d'une transaction de type VERIFICATION dont l'autorisation ou la demande de renseignement a été acceptée. Ce statut ne peut évoluer. Les transactions dont le statut est **Accepté** ne sont jamais remises en banque.
AUTHORISED	**En attente de remise** La transaction est acceptée et sera remise en banque automatiquement à la date prévue.
AUTHORISED_TO_VALIDATE	**À valider** La transaction, créée en validation manuelle, est autorisée. Le marchand doit valider manuellement la transaction afin qu'elle soit remise en banque. La transaction peut être validée tant que la date d'expiration de la demande d'autorisation n'est pas dépassée. Si cette date est dépassée alors le paiement prend le statut **Expiré**. Ce statut est définitif.
CANCELLED	**Annulé** La transaction est annulée par le marchand.
CAPTURED	**Présenté** La transaction est remise en banque.
CAPTURE_FAILED	**La remise de la transaction a échoué.** Contactez le Support.
EXPIRED	**Expiré** Ce statut intervient dans le cycle de vie d'un paiement avec capture différée. La date d'expiration de la demande d'autorisation est atteinte et le marchand n'a pas validé la transaction. Le porteur ne sera donc pas débité.
REFUSED	**Refusé**

Tous droits réservés

Valeur	Description
	La transaction est refusée.
SUSPENDED	**Suspendu** La remise de la transaction est temporairement bloquée par l'acquéreur (AMEX GLOBAL ou SECURE TRADING). Une fois la remise traitée correctement, le statut de la transaction deviendra **CAPTURED**.
UNDER_VERIFICATION	**Vérification en cours** En attente de la réponse de l'acquéreur. Ce statut est temporaire. Pour les transactions CB ou PPRO, ce statut indique qu'un remboursement a été demandé. Des contrôles sont en cours pour valider le remboursement. Une notification sera envoyée au site marchand pour l'avertir du changement de statut. Nécessite l'activation de la règle de notification URL de notification sur modification par batch.
WAITING_AUTHORISATION	**En attente d'autorisation** Le délai de remise en banque est supérieur à la durée de validité de l'autorisation.
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 que la demande d'autorisation et la remise aient lieu.

4. Analysez le champ **vads_occurrence_type** pour déterminer s'il s'agit d'un paiement unitaire ou d'un paiement faisant partie d'une série (abonnement ou paiement en N fois).

Valeur	Description
UNITAIRE	Paiement unitaire (paiement comptant).
RECURRENT_INITIAL	Premier paiement d'une série.
RECURRENT_INTERMEDIAIRE	Énième paiement d'une série.
RECURRENT_FINAL	Dernier paiement d'une série.

5. Analysez le champ **vads_payment_config** pour déterminer s'il s'agit d'un **paiement en N fois**.

Nom du champ	Valeur pour un paiement comptant	Valeur pour un paiement en plusieurs fois
vads_payment_config	SINGLE	MULTI (dont la syntaxe exacte est MULTI:first=X;count=Y;period=Z)

S'il s'agit d'un paiement en N fois, identifiez le numéro de l'échéance en récupérant la valeur du champ **vads_sequence_number**.

Attention : avec l'application du Soft Decline, le champ **vads_sequence_number** ne permet plus d'identifier facilement le premier paiement d'un paiement en N fois. Le premier paiement pouvant prendre un numéro de séquence différent de 1, le numéro de séquence du deuxième paiement ne sera pas forcément 2.

Tous droits réservés

6. Récupérez la valeur du champ **vads_trans_date** pour identifier la date du paiement.

7. Analysez le champ **vads_payment_option_code** pour déterminer s'il s'agit d'un paiement en plusieurs échéances :

Valeur	Description
1	Paiement en 1 échéance
2	Paiement en 2 échéances
3	Paiement en 3 échéances
n	Paiement en n échéances

8. Récupérez la valeur du champ **vads_capture_delay** pour identifier le nombre de jours avant la remise en banque.

   Ceci vous permettra d'identifier s'il s'agit d'un paiement immédiat ou différé.

9. Récupérez le montant et la devise utilisée. Pour cela, récupérez les valeurs des champs suivants :

Nom du champ	Description
vads_amount	Montant du paiement dans sa plus petite unité monétaire.
vads_currency	Code de la devise utilisée pour le paiement.
vads_change_rate	Taux de change utilisé pour calculer le montant réél du paiement (voir vads_effective_amount).
vads_effective_amount	Montant du paiement dans la devise réellement utilisée pour effectuer la remise en banque.
vads_effective_currency	Devise dans laquelle la remise en banque va être effectuée.

10. Récupérez la valeur du champ **vads_auth_result** pour connaître le résultat de la demande d'autorisation.

    La liste complète des codes renvoyés est consultable dans le dictionnaire de données.

    Pour vous aider à comprendre le motif du refus, voici une liste des codes fréquemment retournés :

Valeur	Description
03	**Accepteur invalide** Ce code est émis par l'acquéreur. Il correspond à un problème de configuration sur les serveurs d'autorisation. (ex: contrat clos, mauvais code MCC déclaré, etc..). **Pour connaître la raison précise du refus, le marchand doit contacter sa banque.**
05	**Ne pas honorer** Ce code est émis par la banque émettrice de la carte. Il est utilisé dans les cas suivants : • Date d'expiration invalide, • CVV invalide, • crédit dépassé, • solde insuffisant (etc.) **Pour connaître la raison précise du refus, l'acheteur doit contacter sa banque.**
51	**Provision insuffisante ou crédit dépassé** Ce code est émis par la banque émettrice de la carte. Il peut être obtenu si l'acheteur ne dispose pas d'un solde suffisant pour réaliser son achat. **Pour connaître la raison précise du refus, l'acheteur doit contacter sa banque.**
56	**Carte absente du fichier** Ce code est émis par la banque émettrice de la carte.

Valeur	Description
	Le numéro de carte saisi est erroné ou le couple numéro de carte + date d'expiration n'existe pas.
57	**Transaction non permise à ce porteur** Ce code est émis par la banque émettrice de la carte. Il est utilisé dans les cas suivants : • l'acheteur tente d'effectuer un paiement sur internet avec une carte de retrait, • le plafond d'autorisation de la carte est dépassé. **Pour connaître la raison précise du refus, l'acheteur doit contacter sa banque.**
59	**Suspicion de fraude** Ce code est émis par la banque émettrice de la carte. Il peut être envoyé suite à une saisie répétée de CVV ou de date d'expiration erronée. **Pour connaître la raison précise du refus, l'acheteur doit contacter sa banque.**
60	**L'accepteur de carte doit contacter l'acquéreur** Ce code est émis par l'acquéreur. Il correspond à un problème de configuration sur les serveurs d'autorisation. Il est utilisé lorsque le contrat commerçant ne correspond pas au canal de vente utilisé. (ex : une transaction e-commerce avec un contrat VAD-saisie manuelle). **Contactez le service client pour régulariser la situation.**
81	**Le paiement non sécurisé n'est pas admis par l'émetteur** Ce code est émis par la banque émettrice de la carte. Sur réception de ce code, la plateforme de paiement réalise automatiquement une nouvelle tentative de paiement avec authentification 3-D Secure quand cela est possible.

11. Récupérez le résultat de l'authentification du porteur. Pour cela:

a. Récupérez la valeur du champ **vads_threeds_enrolled** pour déterminer le statut de l'enrôlement de la carte.

Valeur	Description
Vide	Processus 3DS non réalisé (3DS désactivé dans la demande, marchand non enrôlé ou moyen de paiement non éligible au 3DS).
Y	Authentification disponible, porteur enrôlé.
N	Porteur non enrôlé.
U	Impossible d'identifier le porteur ou carte non éligible aux tentatives d'authentification (ex. Cartes commerciales ou prépayées).

b. Récupérez le résultat de l'authentification du porteur en récupérant la valeur du champ **vads_threeds_status**.

Valeur	Description
Vide	Authentification 3DS non réalisée (3DS désactivé dans la demande, porteur non enrôlé ou moyen de paiement non éligible au 3DS).
Y	Porteur authentifié avec succès.
N	Erreur d'authentification du porteur.
U	Authentification impossible.
A	Tentative d'authentification mais authentification non réalisée.

12. Récupérez le résultat des contrôles associés à la fraude en identifiant la valeur du champ **vads_risk_control**. Ce champ est envoyé uniquement si le marchand a:

- souscrit au service "**Aide à la décision**"
- activé au moins un contrôle depuis son Back Office Expert (menu **Paramétrage** > **Contrôle des risques**).

Tous droits réservés

Il prend comme valeur une liste de valeurs séparées par un ";" dont la syntaxe est : **vads_risk_control = control1=result1;control2=result2**

Les valeurs possibles pour **control** sont :

Valeur	Description
CARD_FRAUD	Contrôle la présence du numéro de carte de l'acheteur dans la liste grise de cartes.
SUSPECT_COUNTRY	Contrôle la présence du pays émetteur de la carte de l'acheteur dans la liste des pays interdits.
IP_FRAUD	Contrôle la présence de l'adresse IP de l'acheteur dans la liste grise d'IP.
CREDIT_LIMIT	Contrôle la fréquence et les montants d'achat d'un même numéro de carte, ou le montant maximum d'une commande.
BIN_FRAUD	Contrôle la présence du code BIN de la carte dans la liste grise des codes BIN.
ECB	Contrôle si la carte de l'acheteur est de type e-carte bleue.
COMMERCIAL_CARD	Contrôle si la carte de l'acheteur est une carte commerciale.
SYSTEMATIC_AUTO	Contrôle si la carte de l'acheteur est une carte à autorisation systématique.
INCONSISTENT_COUNTRIES	Contrôle si le pays de l'adresse IP, le pays émetteur de la carte de paiement, et le pays de l'adresse de l'acheteur sont cohérents entre eux.
NON_WARRANTY_PAYMENT	Transfert de responsabilité.
SUSPECT_IP_COUNTRY	Contrôle la présence du pays de l'acheteur, identifié par son adresse IP, dans la liste des pays interdits.

Les valeurs possibles pour **result** sont :

Valeur	Description
OK	OK.
WARNING	Contrôle informatif échoué.
ERROR	Contrôle bloquant échoué.

13. Récupérez le type de carte utilisé pour le paiement.

Deux cas de figures peuvent se présenter:

- Pour un paiement réalisé avec **une seule carte**. Les champs à traiter sont les suivants :

Nom du champ	Description
vads_acquirer_network	Code du réseau acquéreur
vads_card_brand	Marque de la carte utilisée pour le paiement. ex : CB, VISA, VISA_ELECTRON, MASTERCARD, MAESTRO, VPAY
vads_card_number	Numéro masqué du moyen de paiement (carte ou token réseau, IBAN, compte PayPal).

Tous droits réservés

Nom du champ	Description
vads_expiry_month	Mois d'expiration du moyen de paiement.
vads_expiry_year	Année d'expiration du moyen de paiement.
vads_cardholder_card_number	Numéro masqué de la carte utilisée par l'acheteur. Vide si le moyen de paiement utilisé n'est pas une carte.
vads_cardholder_expiry_month	Mois d'expiration de la carte utilisée par l'acheteur. Vide si le moyen de paiement utilisé n'est pas une carte.
vads_cardholder_expiry_year	Année d'expiration de la carte utilisée par l'acheteur. Vide si le moyen de paiement utilisé n'est pas une carte.
vads_bank_code	Code de la banque émettrice
vads_bank_label	Nom de la banque émettrice
vads_bank_product	Code produit de la carte
vads_card_country	Code Pays du pays d'émission de la carte (Code alpha ISO 3166-2 ex : "FR" pour la France, "PF" pour la Polynésie Française, "NC" pour la Nouvelle Calédonie, "US" pour les Etats-Unis.).

- Pour un **paiement complémentaire** (c'est-à-dire une transaction utilisant plusieurs moyens de paiement), les champs à traiter sont les suivants :

Nom du champ	Valeur	Description
vads_card_brand	MULTI	Plusieurs types de cartes sont utilisés pour le paiement.
vads_payment_seq	Au format json, voir détails ci-dessous.	Détails des transactions réalisées.

Le champ **vads_payment_seq** (format json) décrit la séquence du paiement complémentaire. Il contient les éléments :

1. "trans_id" : identifiant de la transaction global à la séquence de paiement.
2. "transaction" : tableau des transactions de la séquence. Les éléments qui le composent sont les suivants :

Nom du paramètre	Description
amount	Montant de la séquence de paiement.
operation_type	Opération de débit.
auth_number	Numéro d'autorisation. Ne sera pas retourné si non applicable au moyen de paiement concerné. Exemple : 949478
auth_result	Code retour de la demande d'autorisation.
capture_delay	Délai avant remise (en jours). • Pour un paiement par carte bancaire, la valeur de ce paramètre tient compte du délai en nombre de jours avant la remise en banque. Si ce paramètre n'est pas transmis dans le formulaire de paiement, la valeur par défaut définie dans le Back Office Expert sera utilisée.
card_brand	Moyen de paiement utilisé. Pour un paiement par carte bancaire (exemple CB ou cartes CB cobadgées Visa ou Mastercard), ce paramètre est valorisé à **"CB"**.

Tous droits réservés

<table>
<tr><th>Nom du paramètre</th><th>Description</th></tr>
<tr><td></td><td>Se référer au guide d'intégration du formulaire de paiement disponible sur notre site documentaire pour visualiser la liste complète des types de carte.</td></tr>
<tr><td>card_number</td><td>Numéro masqué du moyen de paiement (carte ou token réseau, IBAN ou compte PayPal).</td></tr>
<tr><td>expiry_month</td><td>Mois d'expiration du moyen de paiement.</td></tr>
<tr><td>expiry_year</td><td>Année d'expiration du moyen de paiement.</td></tr>
<tr><td>cardholder_card_numb</td><td>Numéro masqué de la carte utilisée par l'acheteur. Vide si le moyen de paiement utilisé n'est pas une carte.</td></tr>
<tr><td>cardholder_expiry_mor</td><td>Mois d'expiration de la carte utilisée par l'acheteur. Vide si le moyen de paiement utilisé n'est pas une carte.</td></tr>
<tr><td>cardholder_expiry_yea</td><td>Année d'expiration de la carte utilisée par l'acheteur. Vide si le moyen de paiement utilisé n'est pas une carte.</td></tr>
<tr><td>payment_certificate</td><td>Certificat de paiement.</td></tr>
<tr><td>contract_used</td><td>Contrat utilisé pour le paiement.</td></tr>
<tr><td>identifier</td><td>Identifiant unique (token/alias) associé à un moyen de paiement.</td></tr>
<tr><td>identifier_status</td><td>Présent uniquement si l’action demandée correspond à la création ou à la mise à jour d'un alias.
Valeurs possibles :
<table><tr><th>Valeur</th><th>Description</th></tr><tr><td>CREATED</td><td>La demande d’autorisation a été acceptée.
L'alias (ou RUM pour un paiement SEPA) est créé avec succès.</td></tr><tr><td>NOT_CREATED</td><td>La demande d’autorisation a été refusée.
L'alias (ou RUM pour un paiement SEPA) n'est pas créé et n'apparaîtra pas dans le Back Office Expert.</td></tr><tr><td>UPDATED</td><td>L'alias (ou RUM pour un paiement SEPA) est mis à jour avec succès.</td></tr><tr><td>NOT_UPDATED</td><td>L'alias (ou RUM pour un paiement SEPA) n'a pas été mis à jour.</td></tr><tr><td>ABANDONED</td><td>Action abandonnée par l'acheteur (débiteur).
L'alias (ou RUM pour un paiement SEPA) n'est pas créé et n'apparaîtra pas dans le Back Office Expert.</td></tr></table></td></tr>
<tr><td>presentation_date</td><td>Pour un paiement par carte bancaire, ce paramètre correspond à la date de remise en banque souhaitée (au format ISO 8601).</td></tr>
<tr><td>trans_id</td><td>Numéro de transaction.</td></tr>
<tr><td>ext_trans_id</td><td>Paramètre absent pour le paiement par carte bancaire.</td></tr>
<tr><td>trans_uuid</td><td>Référence unique générée par la plateforme de paiement suite à la création d'une transaction de paiement.
Offre une garantie d'unicité pour chaque transaction.</td></tr>
<tr><td>extra_result</td><td>Code numérique du résultat des contrôles de risques.
<table><tr><th>Code</th><th>Description</th></tr><tr><td>Vide</td><td>Pas de contrôle effectué.</td></tr></table></td></tr>
</table>

Tous droits réservés

<table>
<tr><th>Nom du paramètre</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Code</th><th>Description</th></tr>
<tr><td>00</td><td>Tous les contrôles se sont déroulés avec succès.</td></tr>
<tr><td>02</td><td>La carte a dépassé l’encours autorisé.</td></tr>
<tr><td>03</td><td>La carte appartient à la liste grise du marchand.</td></tr>
<tr><td>04</td><td>Le pays d’émission de la carte appartient à la liste grise du marchand.</td></tr>
<tr><td>05</td><td>L’adresse IP appartient à la liste grise du marchand.</td></tr>
<tr><td>06</td><td>Le code bin appartient à la liste grise du marchand.</td></tr>
<tr><td>07</td><td>Détection d’une e-carte bleue.</td></tr>
<tr><td>08</td><td>Détection d’une carte commerciale nationale.</td></tr>
<tr><td>09</td><td>Détection d’une carte commerciale étrangère.</td></tr>
<tr><td>14</td><td>Détection d’une carte à autorisation systématique.</td></tr>
<tr><td>20</td><td>Contrôle de cohérence : aucun pays ne correspond (pays IP, pays carte, pays de l’acheteur).</td></tr>
<tr><td>30</td><td>Le pays de l’adresse IP appartient à la liste grise.</td></tr>
<tr><td>99</td><td>Problème technique rencontré par le serveur lors du traitement d’un des contrôles locaux.</td></tr>
</table>
</td></tr>
<tr><td>sequence_number</td><td>Numéro de séquence.</td></tr>
<tr><td>trans_status</td><td>Statut de la transaction.</td></tr>
</table>

Les transactions annulées sont également présentes dans le tableau.

14. Enregistrez le type de wallet qui a servi pour le paiement en récupérant la valeur du champ **vads_wallet**.

    Le champ **vads_wallet** est présent uniquement lorsqu'un wallet est utilisé pour le paiement.

Valeur du champ	Type de wallet
APPLE_PAY	Apple Pay
GOOGLEPAY	Google pay

15. Enregistrez la valeur du champ **vads_trans_uuid**. Elle vous permettra d'identifier de manière unique la transaction si vous utilisez les API Web Services.

16. Récupérez toutes les informations concernant le détail de la commande, le détail de l'acheteur et le détail de la livraison.

    Ces données sont présentes dans la réponse que si elles ont été envoyées dans le formulaire de paiement.

    Leur valeur est identique à celle soumise dans le formulaire.

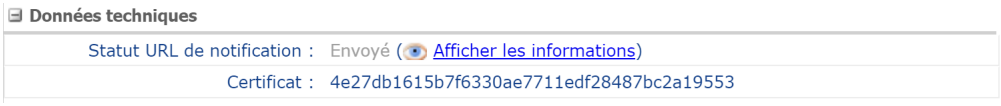
17. Procédez à la mise à jour de la commande.

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).

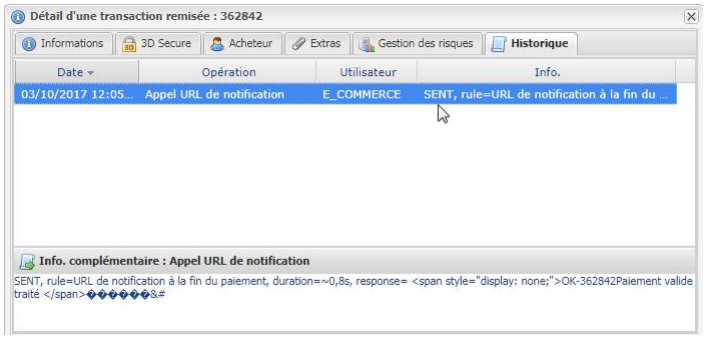
Tous droits réservés

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.

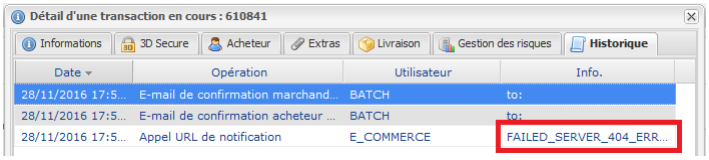
Pour obtenir plus d'informations sur une notification, cliquez sur le lien **Afficher les informations** ou cliquez sur l'onglet **Historique** et recherchez la ligne **Appel URL de notification**.

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. TRAITER LE RETOUR À LA BOUTIQUE

Par défaut, lorsque l'acheteur revient sur le site marchand, aucun paramètre n'est transmis par son navigateur.

Néanmoins si le champ **vads_return_mode** a été transmis dans le formulaire de paiement (voir chapitre **Gérer le retour vers le site marchand**) il sera possible de récupérer les données :

- soit en GET : données présentes dans l'url sous la forme : ?param1=valeur1&param2=valeur2.
- soit en POST : données envoyées dans un formulaire POST.

Les données transmises au navigateur sont les mêmes que lors des notifications (IPN).

Seuls les champs **vads_url_check_src** et **vads_hash** ne seront envoyés que dans la notification instantanée.

Vous pouvez vous référer au chapitre **Analyser le résultat du paiement** pour analyser ces données.

Le retour à la boutique doit vous permettre uniquement d'afficher un contexte visuel à l'acheteur.

Tous droits réservés

16. 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