



Guide d'implémentation

Interface avec la plateforme de paiement

Version 2.1

Rédaction, Vérification, Approbation

Rédaction		Vérification		Approbation	
Nom	Date/Visa	Nom	Date/Visa	Nom	Date/Visa
Lyra-Network	22/02/2010				

Historique du document

Version	Auteur	Date	Commentaires
2.1	Lyra-Network	26/03/2010	Modification documentaire
2.0	Lyra-Network	22/02/2010	Version initiale.

Confidentialité

Toutes les informations contenues dans ce document sont considérées comme confidentielles. L'utilisation de celles-ci en dehors du cadre de cette consultation ou la divulgation à des personnes extérieures est soumise à l'approbation préalable de Lyra Network

SOMMAIRE

1.1 PRINCIPE GENERAL.....	1
1.1. Cinématique des échanges	1
1.2. Sécurité	3
2. REDIRECTION VERS LA PLATEFORME DE PAIEMENT	4
2.1. Format et codage des paramètres	4
2.2. Liste des paramètres.....	5
2.2.1. Format d'échange	5
2.2.2. Description détaillée des paramètres	6
2.3. Signature	12
3. RETOUR VERS LE MARCHAND	13
3.1. Retour vers le site marchand	13
3.1.1. Liste des paramètres	13
3.1.2. Signature	17
3.2. Réponse de serveur à serveur (Réponse systématique) ...	18
4. COMMENT ACTIVER LA BOUTIQUE EN PRODUCTION ?	19
4.1. Récupération du certificat de test et de l'identifiant du site (site_ID)	19
4.2. Réalisation des paramétrages de la boutique	20
4.3. Phase de test & Cartes à utiliser	21
4.4. Transmission du PV de recette	22
4.5. Activation de la boutique en production	23
4.5.1. Récupération du certificat de production et modification du champ « ctx_mode »	23
4.5.2. Réalisation d'une première transaction en production.....	23
5. ASSISTANCE TECHNIQUE.....	24
6. Acronymes et glossaire	25
6.1. Acronymes	25
6.2. Glossaire	25
7. ANNEXES	28
7.1. Exemples d'implémentation	28
7.1.1. CONTROLE DE LA SIGNATURE (Java)	28
7.1.2. Acquisition des données carte déléguées à la plateforme (PHP)	30
7.1.3. Acquisition des données carte par le commerçant (PHP)	31
7.1.4. Acquisition des données carte par le commerçant (PHP)	32
7.2. Pages standards de la plateforme de paiement.....	34
7.3. Personnalisation des pages de paiement à l'aide du paramètre « vads_theme_config ».....	37
7.3.1. Principe de fonctionnement.....	37
7.3.2. Exemple d'utilisation.....	38

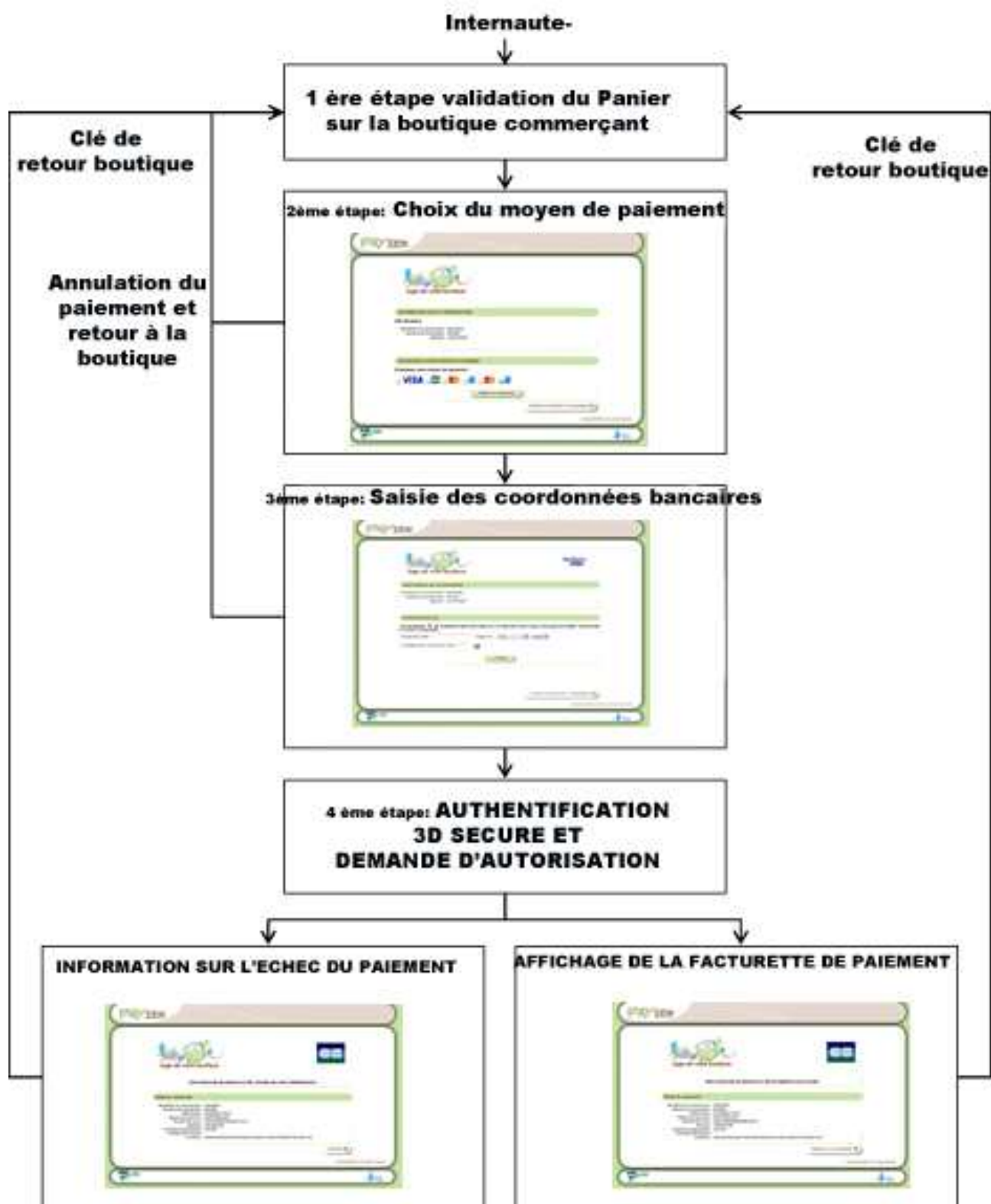
1. PRINCIPE GENERAL

1.1. Cinématique des échanges

La cinématique d'échange est la suivante :

- 1) Une fois la commande de l'internaute finalisée, le site marchand redirige celui-ci vers la plateforme de paiement. Cette redirection prendra la forme d'un formulaire HTTP POST en HTTPS contenant des paramètres décrits dans le chapitre 2.2.1
- 2) La plateforme de paiement, après vérification des paramètres et de leur signature, présentera soit une page de sélection du type de carte, soit directement la saisie correspondante à la carte lorsqu'il n'y a pas d'ambiguïté ou lorsque le moyen de paiement a été forcé dans le formulaire.
- 3) La plateforme de paiement affichera une page de saisie de numéro de carte, date d'expiration et cryptogramme visuel. En cas de validation, une authentification 3D-Secure aura éventuellement lieu, puis une demande d'autorisation sera effectuée auprès de la banque du client, en plus des contrôles de fraude internes de la plateforme de paiement.
- 4) Une page de résumé sera présentée en cas de succès ou d'échec, avec un bouton de retour vers le site marchand.

Vu de l'internaute, la cinématique de paiement est représentée sur le schéma ci-dessous :



1.2. Sécurité

Dans la communication entre la plateforme de paiement et le site marchand, un mécanisme de signature est à mettre en place. Les échanges étant effectués par paramètres de formulaire, l'un de ces paramètres sera la signature.

La signature sera générée comme suit :

- Création d'une chaîne de caractère représentant la concaténation de valeurs de certaines données du formulaire, séparées par le caractère " + ".
- Ajout à cette chaîne d'un " certificat " numérique (de test ou de production selon le contexte).
- Hachage de la chaîne résultante avec l'algorithme SHA1.

La plateforme de paiement effectuera obligatoirement la vérification de la signature. Il est de la responsabilité du commerçant de vérifier à son tour les données transmises en retour, notamment pour mettre en œuvre un mécanisme de validation de commande.

2. REDIRECTION VERS LA PLATEFORME DE PAIEMENT

Cette redirection est effectuée via un formulaire HTTP POST. Le formulaire contient des champs décrits ci-dessous, ainsi qu'une signature basée sur une partie de ces champs. L'URL de la plateforme de paiement est la suivante :

<https://secure.payzen.eu/vads-payment/>

2.1. Format et codage des paramètres

Aux chapitres suivants, les paramètres et leur format sont listés dans des tableaux, dont voici la légende :

- **Nom** : indique le nom du paramètre, tel qu'ils seront utilisés dans les requêtes HTTP.

- **Format** : indique le format des données, selon la codification suivante :

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
3	Longueur fixe de 3 caractères
...12	Longueur variable jusqu'à 12 caractères

- **Exemple** : représente un exemple de codage correct des données.

- **Présence Obligatoire** : indique si la présence du paramètre est obligatoire. *Attention, un paramètre obligatoire peut être vide.*

Notation	Signification
X	Obligatoire
C	Conditionnel : la condition rendant ce paramètre obligatoire est précisée par une note
F	Facultatif
.	Non avenu

- **Code** : en cas d'erreur dans l'interfaçage entre le site marchand et la plateforme de paiement, cette dernière indiquera par un code numérique le paramètre fautif dans le champ vads_extra_result (cf. §3.1.1).

2.2. Liste des paramètres

2.2.1. Format d'échange

Nom	Format	Code	Obligatoire
vads_action_mode		47	X
vads_amount	n..12	09	X
vads_capture_delay	n..3	06	F
vads_contrib	ans..255	31	F
vads_currency	n3	10	X
vads_cust_address	an..255	19	F
vads_cust_country	a2	22	F
vads_cust_email	an..127	15	C(1)
vads_cust_id	an..63	16	F
vads_cust_name	an..127	18	F
vads_cust_phone	an..63	23	F
vads_cust_title	an..63	17	F
vads_cust_city	an..63	21	F
vads_cust_zip	an..63	20	F
vads_ctx_mode		11	X
vads_language	a2	12	F
vads_order_id	an..12	13	F
vads_order_info	an..255	14	F
vads_order_info2	an..255	14	F
vads_order_info3	an..255	14	F
vads_page_action		46	X
vads_payment_cards	an..127	08	F
vads_payment_config		07	X
signature	an40		X
vads_return_mode		48	C(2)
vads_site_id	n8	02	X
vads_theme_config	ans..255	32	F
vads_trans_date	n14	04	X
vads_trans_id	n6	03	X
vads_validation_mode	n..1	05	F
vads_version		01	X
vads_url_success	ans..127	24	F
vads_url_referral	ans..127	26	F
vads_url_refused	ans..127	25	F
vads_url_cancel	ans..127	27	F
vads_url_error	ans..127	29	F
vads_url_return	ans..127	28	F
vads_user_info	ans..255	61	.
vads_contracts	ans..255	62	C(3)

- C(1) Obligatoire si souscription à l'envoi d'e-mail de confirmation de paiement au client
- C(2) Obligatoire si souhait du commerçant de recevoir la réponse à la demande sur l'URL internet de retour boutique en formulaire GET ou POST (après clic internaute sur bouton retour boutique).
Ce paramétrage n'impacte pas la transmission, ni les paramètres de transfert, de la réponse de serveur à serveur (URL serveur commerçant).
- C(3) Obligatoire si le numéro de contrat commerçant à utiliser n'est pas celui configuré par défaut sur la plateforme de paiement

2.2.2. Description détaillée des paramètres

signature

Paramètre **obligatoire** permettant à la plateforme de vérifier la validité de la requête transmise (voir chapitre 2.3).

vads_action_mode

Paramètre **obligatoire** indiquant le mode de fonctionnement de la plateforme :

- **SILENT** : correspond au cas où l'acquisition des données carte est effectuée par le commerçant.
- **INTERACTIVE** : correspond au cas où l'acquisition des données carte est déléguée à la plateforme.

vads_amount

Paramètre **obligatoire**. Montant de la transaction exprimé en son unité indivisible (en cents pour l'Euro).

Exemple : pour une transaction de 10 euros et 28 centimes, la valeur du paramètre est 1028.

Attention : Un montant à zéro ou incorrect (présence de décimales) génère un message d'incident technique associé à un code retour (vads_extra_result) valorisé à 09.

vads_capture_delay

Paramètre *facultatif* indiquant le délai en nombre de jours avant remise en banque. Si ce paramètre n'est pas transmis, alors la valeur par défaut sera utilisée. Cette dernière est paramétrable dans le back office Payzen par toutes les personnes dûment habilitées.

vads_contracts

Paramètre *facultatif* permettant de spécifier pour chaque réseau d'acceptation, le contrat commerçant à utiliser. Le formalisme du paramètre est le suivant :

RESEAU1=contratReseau1;RESEAU2=contratReseau2;RESEAU3=contratReseau3

Les différents réseaux possibles étant :

Réseau	Valorisation 'vads_contracts'
American Express	AMEX
CB	CB

Par exemple, si vous disposez d'un 2ème contrat VAD de numéro 12312312 dans votre banque, et que vous souhaitez enregistrer pour une commande donnée un paiement par carte bancaire (Visa, MasterCard ou CB) sur ce contrat, alors il faudra valoriser **vads_contracts** de la manière suivante :

CB=12312312

Remarque : ce paramètre est facultatif et n'est utile que dans le cas où vous avez plusieurs contrats VAD sur le même réseau et si vous souhaitez en changer dynamiquement en fonction du paiement. Si ce paramètre n'est pas renseigné ou absent, alors le paiement sera enregistré sur votre contrat commerçant VAD par défaut.

vads_contrib

Information complémentaire *facultative* destinée à indiquer le nom de la contribution utilisée lors du paiement (joomla, oscommerce...). Si vous utilisez une implémentation propriétaire, ce champ peut accueillir votre numéro de version interne, par exemple.

vads_ctx_mode

Paramètre **obligatoire** indiquant le mode de sollicitation de la plateforme de paiement :

- **TEST** : utilisation du mode test, nécessite d'employer le certificat de test pour la signature.
- **PRODUCTION** : utilisation du mode production, nécessite d'employer le certificat de production pour la signature.

vads_currency

Paramètre **obligatoire** indiquant la monnaie à utiliser, selon la norme ISO 4217 (code numérique).

http://www.iso.org/iso/support/currency_codes_list-1.htm

Pour l'Euro, la valeur est 978.

vads_cust_address

Paramètre *facultatif*. Adresse postale du client

vads_cust_city

Paramètre *facultatif*. Ville du client

vads_cust_country

Paramètre *facultatif*. Code pays du client à la norme ISO 3166.

http://www.iso.org/iso/english_country_names_and_code_elements

Pour la France, le code est FR.

vads_cust_email

Paramètre *facultatif*. Adresse e-mail du client, nécessaire pour lui envoyer un mail récapitulatif de la transaction.

vads_cust_id

Paramètre *facultatif*. Identifiant du client chez le marchand.

vads_cust_name

Paramètre *facultatif*. Nom du client

vads_cust_phone

Paramètre *facultatif*. Numéro de téléphone du client

vads_cust_title

Paramètre *facultatif*. Civilité du client

vads_cust_zip

Paramètre *facultatif*. Code postal du client

vads_language

Paramètre *facultatif*. Langue dans laquelle doit être affichée la page de paiement (norme ISO 639-1).

Les langues possibles sont les suivantes :

Langue	Codification ISO 639-1
Allemand	de
Anglais	en
Chinois	zh
Espagnol	es
Français	fr
Italien	it
Japonais	jp

Par défaut, le français est sélectionné.

vads_order_id

Paramètre *facultatif*. Numéro de commande qui pourra être rappelé dans l'e-mail de confirmation de paiement adressé au client.

vads_order_info, vads_order_info2, vads_order_info3

Champs libres *facultatifs* pouvant par exemple servir à stocker un résumé de la commande.

vads_page_action

Ce paramètre est **obligatoire** et doit être valorisé à **PAYMENT**.

vads_payment_cards

Ce paramètre *facultatif* contient la liste des types de cartes à proposer à l'internaute, séparés par des " ;".

Si la liste ne contient qu'un type de carte, la page de saisie des données du paiement sera directement présentée. Sinon la page de sélection du moyen de paiement sera présentée.

Si ce paramètre est vide alors l'ensemble des moyens de paiement défini dans l'outil de gestion de caisse sera présenté en sélection. Par défaut **la valeur VIDE est conseillée**.

Les différents réseaux possibles sont :

Réseau de la carte	Valorisation 'payment_cards'
Amex	AMEX
CB	CB
Eurocard / MasterCard	MASTERCARD
Visa	VISA
Maestro	MAESTRO
e-carte bleue	E-CARTEBLEUE

vads_payment_config

Ce paramètre **obligatoire** indique le type du paiement :

- **SINGLE** indique un paiement unitaire.
- **MULTI** indique un paiement en plusieurs fois. Dans ce cas, le paramètre est constitué de la chaîne « MULTI: », suivi par des paires clés/valeurs séparées par des « ; ». Les paramètres sont les suivants :
 - o « first » indique le montant du premier paiement.
 - o « count » indique le nombre de paiements total.
 - o « period » indique l'intervalle en nombre de jours entre 2 paiements.

Exemple:

```
vads_currency=978  
vads_amount=10000  
vads_payment_config=MULTI:first=5000;count=3;period=30
```

Dans cette configuration :

- Le montant total de l'achat est de 100 euros,
- Un premier paiement de 50 euros sera effectué à aujourd'hui + « vads_capture_delay » jours.
- Un deuxième paiement de 25 euros sera effectué à aujourd'hui + « vads_capture_delay » + 30 jours.
- Un troisième et dernier paiement de 25 euros sera effectué à aujourd'hui + « vads_capture_delay » + 60 jours.

Le total des 3 transactions fait bien sûr 100 euros au final.

NB : si la date de validité de la carte ne permet pas de réaliser le ou les dernier(s) paiement(s), en cas d'acquisition des données de la carte sur la plateforme, l'internaute verra sa demande refusée avec le message « date d'expiration invalide », en cas d'acquisition chez le commerçant, le paiement sera refusé avec valorisation du champ **vads_result** à 05.

vads_return_mode

Paramètre permettant de conditionner le passage des paramètres aux URL de retour vers le site marchand.

- **Non défini, vide ou NONE** : aucun paramètre ne sera passé à l'URL de retour.
- **POST** : les paramètres de retour seront transmis à l'URL de retour sous la forme d'un formulaire HTTP POST.
- **GET** : les paramètres de retour seront transmis à l'URL de retour sous la forme d'un formulaire HTTP GET (dans la « query string »).

vads_site_id

Paramètre **obligatoire** attribué lors de l'inscription à la plateforme de paiement.

Sa valeur est consultable sur l'interface de l'outil de gestion de caisse dans l'onglet « Paramétrages » / « Boutique » par toutes les personnes habilitées.

vads_theme_config

Paramètre permettant de personnaliser certains paramètres de la page de paiement standard de la plateforme, comme les logos, bandeaux ainsi que certains messages. Se reporter à l'annexe pour plus d'informations.

vads_trans_date

Ce paramètre est **obligatoire**. Correspond à la date locale du site marchand au format AAAAMMJJHHMMSS.

vads_trans_id

Ce paramètre est **obligatoire**. Il est constitué de 6 caractères numériques et doit être unique pour chaque transaction pour une boutique donnée sur la journée. En effet l'identifiant unique de transaction au niveau de la plateforme de paiement est constitué du **vads_site_id**, de **vads_trans_date** restreint à la valeur de la journée (partie correspondant à AAAAMMJJ) et de **vads_trans_id**. Il est à la charge du site marchand de garantir cette unicité sur la journée. Il doit être **impérativement** compris entre 000000 et 899999. La tranche 900000 et 999999 est **interdite**.

Remarque : une valeur de longueur inférieure à 6 provoque une erreur lors de l'appel à l'URL de paiement. Merci de respecter cette longueur de 6 caractères.

vads_validation_mode

Paramètre précisant le mode de validation de la transaction (manuellement par le commerçant, ou automatiquement par la plateforme).

Valorisation 'vads_validation_mode'	Signification
Absent ou vide	Configuration par défaut de la boutique retenue (paramétrable dans l'outil de gestion de caisse)
0	Validation automatique
1	Validation manuelle

vads_version

Paramètre **obligatoire** et devant être valorisé à **V2**.

vads_url_cancel

Paramètre *facultatif*. Dans le cas où l'acquisition des données bancaires est déléguée à la plateforme de paiement, URL où sera redirigé le client si celui-ci appuie sur " annuler et retourner à la boutique " avant d'avoir procédé au paiement.

vads_url_error

Paramètre *facultatif*. Dans le cas où l'acquisition des données bancaires est déléguée à la plateforme de paiement, URL où sera redirigé le client en cas d'erreur de traitement interne.

vads_url_referral

Paramètre *facultatif*. Dans le cas où l'acquisition des données bancaires est déléguée à la plateforme de paiement, URL où sera redirigé le client en cas de refus d'autorisation avec le code 02 « contacter l'émetteur de la carte », après appui du bouton " retourner à la boutique ".

vads_url_refused

Paramètre *facultatif*. Dans le cas où l'acquisition des données bancaires est déléguée à la plateforme de paiement, URL où sera redirigé le client en cas de refus pour toute autre cause que le refus d'autorisation de motif 02 (contacter l'émetteur de la carte), après appui du bouton " retourner à la boutique ".

vads_url_success

Paramètre *facultatif*. Dans le cas où l'acquisition des données bancaires est déléguée à la plateforme de paiement, URL où sera redirigé le client en cas de succès du paiement, après appui du bouton " retourner à la boutique ".

vads_url_return

Paramètre *facultatif*. Dans le cas où l'acquisition des données bancaires est déléguée à la plateforme de paiement, URL où sera redirigé par défaut le client après un appui sur le bouton " retourner à la boutique ", si les URL correspondantes aux cas de figure vus précédemment ne sont pas renseignées.

Si cette URL n'est pas présente dans la requête, alors c'est la configuration dans l'outil de gestion de caisse qui sera prise en compte.

En effet il est possible de configurer des URL de retour, en mode TEST et en mode PRODUCTION. Ces paramètres sont nommés « URL de retour de la boutique » et « URL de retour de la boutique en mode test » respectivement, et sont accessibles dans l'onglet « Configuration » lors du paramétrage d'une boutique.

Si toutefois aucune URL n'est présente, que ce soit dans la requête ou dans le paramétrage de la boutique, alors le bouton « retourner à la boutique » redirigera vers l'URL générique de la boutique (paramètre nommé « URL » dans la configuration de la boutique).

2.3. Signature

La signature sera constituée de l'intégralité des champs dont le nom commence par la chaîne « vads_ ». Les champs doivent être triés par ordre alphabétique.

Dans le calcul de la signature, l'ordre alphabétique des paramètres doit être respecté.

Les valeurs de ces champs doivent être concaténées entre elles avec le caractère « + ».

Au résultat de cette concaténation, on concatènera la valeur du certificat employé (certificat de test ou de production).

Exemple : si les paramètres de la requête sont les suivants :

- vads_version = V2
- vads_page_action = PAYMENT
- vads_action_mode = INTERACTIVE
- vads_payment_config = SINGLE
- vads_site_id = 12345678
- vads_ctx_mode = TEST
- vads_trans_id = 654321
- vads_trans_date = 20090501193530
- vads_amount = 1524
- vads_currency = 978

et valeur du certificat en fonction du mode =1122334455667788

L'ordre **alphabétique** des paramètres est le suivant : 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.

Il faudra rajouter à ces paramètres la valeur du certificat.

La chaîne à utiliser pour le hachage à l'aide de l'algorithme SHA-1 sera donc la suivante :
INTERACTIVE+1524+TEST+978+PAYMENT+SINGLE+12345678+20090501193530+654321+V2+1122334455667788

Remarque :

La signature à transmettre n'est pas égale à cette chaîne, mais au hachage de cette chaîne à l'aide de l'algorithme SHA-1.

3. RETOUR VERS LE MARCHAND

3.1. Retour vers le site marchand

Le comportement de cette redirection dépend de la valeur du paramètre **vads_return_mode**. Si **vads_return_mode** est valorisé à vide ou **NONE**, aucun paramètre n'est passé en retour vers le site marchand.

Sinon, si **vads_return_mode** est valorisé à **POST** ou **GET**, des paramètres de retour sont passés respectivement sous la forme d'un formulaire HTTP POST, ou dans les paramètres de la « query string ».

Le formulaire contient des champs décrits ci-dessous, ainsi qu'une signature basée sur la totalité de ces champs. Le " certificat " employé est le même que celui de la requête.

3.1.1. Liste des paramètres

Nom	Format	Obligatoire	Remarques
vads_action_mode		oui	idem requête
vads_amount		oui	idem requête
vads_auth_result	n2	oui	vide si erreur avant autorisation
vads_auth_mode		oui	MARK : prise d'empreinte FULL : autorisation du montant total (ou du montant initial dans le cas du paiement en N fois)
vads_auth_number	n6	oui	vide si autorisation échouée.
vads_capture_delay	n..3	oui	valeur par défaut ou valeur spécifiée dans requête
vads_card_brand	an..127	oui	vide si aucune carte n'a été sélectionnée (retour à la boutique).
vads_card_number	an..19	oui	numéro masqué
vads_ctx_mode		oui	idem requête
vads_currency		oui	idem requête
vads_extra_result	n2	oui	numérique, peut être vide.
vads_payment_config	oui	oui	idem requête
Signature		oui	
vads_site_id	oui	oui	idem requête
vads_trans_date	oui	oui	idem requête
vads_trans_id	oui	oui	idem requête
vads_validation_mode	n1	oui	valeur par défaut ou valeur spécifiée dans la requête
vads_warranty_result		oui	vide ou YES, NO, UNKNOWN
vads_payment_certificate	an40	oui	vide si paiement échoué
vads_result	n2	oui	numérique, toujours renseigné
vads_version		oui	Idem requête
vads_order_id			Idem requête
vads_order_info			Idem requête

vads_order_info2			Idem requête
vads_order_info3			Idem requête
vads_cust_address			Idem requête
vads_cust_country			Idem requête
vads_cust_email			Idem requête
vads_cust_id			Idem requête
vads_cust_name			Idem requête
vads_cust_phone			Idem requête
vads_cust_title			Idem requête
vads_cust_city			Idem requête
vads_cust_zip			Idem requête
vads_language			valeur par défaut ou valeur spécifiée dans requête
vads_payment_src			Idem requête
vads_user_info			Idem requête
vads_theme_config			Idem requête
vads_contract_used	ans..250		Contrat utilisé
vads_expiry_month	n..2		Idem requête
vads_expiry_year	n4		Idem requête
vads_card_info	ans..250		Idem requête
vads_card_options	ans..250		Idem requête
vads_threeds_enrolled	a1		
vads_threeds_cavv	ans28		
vads_threeds_eci	n2		
vads_threeds_xid	ans28		
vads_threeds_cavvAlgorithm	n1		
vads_threeds_status	a1		

vads_action_mode, vads_amount, vads_currency, vads_payment_config, vads_site_id, vads_trans_date, vads_trans_id, vads_version, vads_payment_src, vads_user_info, vads_theme_config, vads_order_info, vads_order_info2, vads_order_info3, vads_cust_address, vads_cust_country, vads_cust_email, vads_cust_id, vads_cust_name, vads_cust_phone, vads_cust_title, vads_cust_city, vads_cust_zip, vads_expiry_month, vads_expiry_year, vads_card_info, vads_card_options
Mêmes valeur que la requête.

vads_threeds_enrolled, vads_threeds_cavv, vads_threeds_eci, vads_threeds_xid, vads_threeds_cavvAlgorithm, vads_threeds_status
Mêmes valeurs que la requête si l'authentification 3D-Secure est réalisée par le site marchand. Sinon, ces champs sont valorisés par le résultat de l'authentification 3D-Secure faite via le MPI de la plateforme Payzen.

vads_auth_result

Code retour de la demande d'autorisation retournée par la banque émettrice, si disponible (vide sinon).

auth_result	Signification
00	transaction approuvée ou traitée avec succès
02	contacter l'émetteur de carte
03	accepteur invalide
04	conserver la carte
05	ne pas honorer
07	conserver la carte, conditions spéciales
08	approuver après identification
12	transaction invalide
13	montant invalide
14	numéro de porteur invalide
30	erreur de format
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
51	provision insuffisante ou crédit dépassé
54	date de validité de la carte dépassée
56	carte absente du fichier
57	transaction non permise à ce porteur
58	transaction interdite au terminal
59	suspicion de fraude
60	l'accepteur de carte doit contacter l'acquéreur
61	montant de retrait hors limite
63	règles de sécurité non respectées
68	réponse non parvenue ou reçue trop tard
90	arrêt momentané du système
91	émetteur de cartes inaccessible
96	mauvais fonctionnement du système
94	transaction dupliquée
97	échéance de la temporisation de surveillance globale
98	serveur indisponible routage réseau demandé à nouveau
99	incident domaine initiateur

vads_auth_number

Numéro d'autorisation retourné par le serveur bancaire, si disponible (vide sinon).

vads_auth_mode

Indique comment a été réalisée la demande d'autorisation. Ce champ peut prendre les valeurs suivantes :

- **FULL** : correspond à une autorisation du montant total de la transaction dans le cas d'un paiement unitaire avec remise à moins de 6 jours, ou à une autorisation du montant du premier paiement dans le cas du paiement en N fois, dans le cas d'une remise de ce premier paiement à moins de 6 jours.

- **MARK** : correspond à une prise d'empreinte de la carte, dans le cas où le paiement est envoyé en banque à plus de 6 jours.

vads_capture_delay

Identique à la requête si il a été spécifié dans celle-ci, sinon retourne la valeur par défaut configurée.

vads_card_brand

Type de carte utilisé pour le paiement, si disponible (vide sinon).

vads_card_number

Numéro de carte masqué.

vads_expiry_month

Identique à la requête si il a été spécifié dans celle-ci, sinon retourne le mois d'expiration de la carte utilisée pour le paiement, si disponible (vide sinon).

vads_expiry_year

Identique à la requête si il a été spécifié dans celle-ci, sinon retourne l'année d'expiration de la carte utilisée pour le paiement, si disponible (vide sinon).

vads_language

Identique à la requête si il a été spécifié dans celle-ci, sinon retourne la valeur par défaut configurée.

signature

Paramètre permettant au site marchand de vérifier la validité de la requête transmise par la plateforme de paiement (voir le chapitre suivant).

vads_validation_mode

Identique à la requête si il a été spécifié dans celle-ci, sinon retourne la valeur par défaut configurée.

vads_warranty_result

Si l'autorisation a été réalisée avec succès, indique la garantie du paiement, liée à 3D-Secure :

warranty_result	Signification
YES	Le paiement est garanti
NO	Le paiement n'est pas garanti
UNKNOWN	Suite à une erreur technique, le paiement ne peut pas être garanti
Non valorisé	Garantie de paiement non applicable

vads_payment_certificate

Si l'autorisation a été réalisée avec succès, la plateforme de paiement délivre un certificat de paiement. Pour toute question concernant un paiement réalisé sur la plateforme, cette information devra être communiquée.

vads_result

Code retour général. Est l'une des valeurs suivantes :

- 00 : Paiement réalisé avec succès.
- 02 : Le commerçant doit contacter la banque du porteur.
- 05 : Paiement refusé.
- 17 : Annulation client.
- 30 : Erreur de format de la requête. A mettre en rapport avec la valorisation du champ
- **vads_extra_result.**
- 96 : Erreur technique lors du paiement.

vads_extra_result

Code complémentaire de réponse. Sa signification dépend de la valeur renseignée dans vads_result.

Lorsque vads_result vaut 30 (erreur de requête), alors vads_extra_result contient le code numérique du champ qui comporte une erreur de valorisation ou de format. Cette valeur peut être renseignée à 99 dans le cas d'une erreur inconnue dans la requête.

Lorsque vads_result vaut 05 (refusée) ou 00 (acceptée), alors vads_extra_result contient le code numérique du résultat des contrôles risques.

extra_result	Signification
vide	Pas de contrôle effectué
00	Tous les contrôles se sont déroulés avec succès
02	La carte a dépassé l'encours autorisé
03	La carte appartient à la liste grise du commerçant
04	Le pays d'émission de la carte appartient à la liste grise du commerçant ou le pays d'émission de la carte n'appartient pas à la liste blanche du commerçant.
05	L'adresse IP appartient à la liste grise du commerçant
99	Problème technique rencontré par le serveur lors du traitement d'un des contrôles locaux

3.1.2. Signature

Pour les URL de retour passées en paramètre, la construction de la signature de retour est similaire à celle effectuée lors de la requête. Se référer au chapitre 2.3 pour plus d'informations.

3.2. Réponse de serveur à serveur (Réponse systématique)

Cette fonctionnalité permet de spécifier une **URL sur l'outil de gestion de caisse** que la plateforme de paiement peut **systématiquement** appeler. Contrairement au cas précédent, la requête HTTP ne passe pas par l'intermédiaire du navigateur du client, mais est réalisée **de serveur à serveur**. Elle contient tous les paramètres de réponse décrits au paragraphe 3.1 plus un **paramètre supplémentaire** nommé **vads_hash**.

Remarque importante :

Cette URL est systématiquement appelée avec un formulaire **HTTP POST**, et ce quelque soit la valeur du paramètre **vads_return_mode**.

Attention :

L'utilisation de la réponse de serveur à serveur, via le paramétrage de l'URL correspondante dans le back office Payzen, est fortement conseillée.

Pour le commerçant, c'est le seul moyen de connaître de façon certaine le dénouement de la transaction, et donc de gérer automatiquement ses stocks par exemple.

Seuls les ports **http (80)** et **https (443)** sont disponibles.

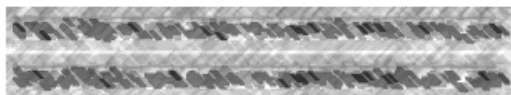
Pour paramétrer cette réponse, aller dans l'outil de gestion de caisse, menu **Paramétrage / boutique / Configuration**, et renseigner la section « **URL serveur** » :

URL serveur

Cette URL est systématiquement appelée à la fin du paiement, réussi ou refusé. Il est indispensable de la renseigner et l'exploiter lorsqu'elle est appelée, si vous voulez analyser les codes retour du paiement et mettre éventuellement à jour votre application.

URL serveur de la boutique en mode test:

URL serveur de la boutique:



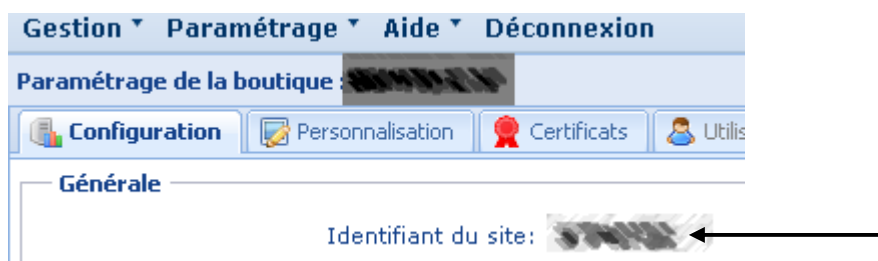
4. COMMENT ACTIVER LA BOUTIQUE EN PRODUCTION ?

4.1. Récupération du certificat de test et de l'identifiant du site (site_ID)

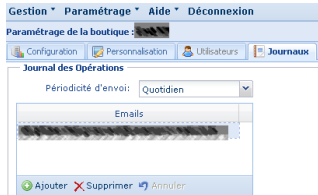
Un « **certificat** » spécifique à la phase de test est nécessaire pour dialoguer avec le serveur de test de la plateforme de paiement.


Il est mis à disposition de toutes les personnes habilitées à la consultation des certificats dans l'outil de gestion de caisse à l'emplacement suivant : **Paramétrage / Boutique / Certificats**.

L'identifiant de site (donnée '**vads_site_id**'), qui a été automatiquement attribué par la plateforme de paiement à votre boutique lors de son inscription, est quant à lui disponible dans l'outil de gestion de caisse à l'emplacement suivant : **Paramétrage / Boutique / Configuration générale**, rubrique « **identifiant de site** ». Cette valeur est à utiliser dans le calcul de la signature.



4.2. Réalisation des paramétrages de la boutique

Élément à paramétrer	Où ?	Comment ?	A quoi cela sert-il ?
Délai de présentation en banque (valeur par défaut pour la boutique)	Outil de gestion de caisse Paramétrage / boutique / configuration Délai de capture: <input type="text" value="0"/> jour(s)	Cf. manuel utilisateur outil de gestion de caisse	Utilisé si le champ « vads_capture_d elay » n'est pas renseigné dans la requête.
Mode de validation (valeur par défaut pour la boutique)	Outil de gestion de caisse Paramétrage / boutique / configuration Mode de validation: <div>Automatique Automatique Manuel</div>	Cf. manuel utilisateur outil de gestion de caisse	Utilisé si le champ « vads_validation_ mode » n'est pas renseigné dans la requête.
URL serveur à configurer en Production et en Test	Outil de gestion de caisse Paramétrage / boutique / configuration Cf. § Erreur ! Source du renvoi introuvable.	Cf. manuel utilisateur outil de gestion de caisse	Utilisé pour la réponse de serveur à serveur
URL de retour A configurer en Production et en Test	Outil de gestion de caisse Paramétrage / boutique / configuration URL de retour de la boutique en mode test: <input type="checkbox"/> URL de retour de la boutique: <input type="checkbox"/>	Cf. manuel utilisateur outil de gestion de caisse	URL où est redirigée l'internaute dans le cas où la requête de paiement est mal formatée
Mode de réception des journaux -> Journal des opérations -> Journal des transactions -> Journal de rapprochement bancaire (réservé aux commerçants ayant souscrit à cette option)	Outil de gestion de caisse Paramétrage / boutique / journaux 	Modifier les critères comme souhaité, puis cliquer sur Sauvegarder. Cf. manuel utilisateur outil de gestion de caisse	Permet de définir la fréquence et les destinataires des journaux de reporting pré- formatés
Libellé de la boutique	Outil de gestion de caisse Paramétrage / boutique / configuration Libellé * :	Modifier le libellé de la boutique, puis cliquer sur Sauvegarder. Cf. manuel e-mail de confirmation de commande	Nom de la boutique tel qu'il apparaîtra sur les e-mail de confirmation de commande (commerçant et/ou client)
Logo et favicon de la boutique	Outil de gestion de caisse Paramétrage / boutique / personnalisation	Cf.. Manuel_utilisateur_ personnalisation_lo go_favicon	Après téléchargement, le logo apparaît sur les pages de paiement et dans le cas où la réception d'e-mail de commande (internaute et/ou commerçant) est activé, dans les entêtes de message.

Élément à paramétrer	Où ?	Comment ?	A quoi cela sert-il ?
E-mails de confirmation de commande (envoi commerçant)	Outil de gestion de caisse Paramétrage / boutique / configuration <small>Envoi d'un e-mail de confirmation de commande au commerçant : <input checked="" type="checkbox"/></small> <small>E-mail commerçant de destination: </small>	Sélectionner la case à cocher, puis renseigner l'adresse e-mail. Cliquer enfin sur Sauvegarder. Cf. manuel e-mail de confirmation de commande	Permet au commerçant de recevoir un mail à chaque commande réalisée avec succès sur sa boutique.
E-mails de confirmation de commande (envoi client) <small>(réservé aux commerçants ayant souscrit à cette option)</small>	-	Demander l'activation au chargé de clientèle. Cf. manuel e-mail de confirmation de commande <small>Envoi d'un e-mail de confirmation de commande au client : <input checked="" type="checkbox"/></small>	Permet aux clients de recevoir un mail à chaque commande réalisée sur la boutique.
Module d'aide à la décision <small>(réservé aux commerçants ayant souscrit à cette option)</small>	Outil de gestion de caisse Paramétrage / boutique / contrôle risques	Demander l'activation au chargé de clientèle, puis effectuer le paramétrage tel que décrit dans le manuel module d'aide à la décision	Permet de paramétrer les différents contrôles du module anti-fraude.

4.3. Phase de test & Cartes à utiliser

Préalablement au passage en production de la boutique, il est nécessaire de réaliser des tests pour s'assurer du bon dialogue entre le site marchand et la plateforme de paiement.

Ces tests doivent impérativement être réalisés avant de demander le passage en production.

Les demandes de paiement de test adressées via le formulaire HTTP POST doivent contenir la donnée **vads_ctx_mode** valorisée à **TEST**. Elles doivent également **utiliser le certificat de test** précédemment récupéré pour le calcul de la signature.

En phase de test, le commerçant peut tester les configurations 3D-Secure ou non 3D-Secure, quelle que soit sa configuration réelle

Différents cas de paiement peuvent être simulés **en utilisant les numéros de carte de test précisés ci-dessous ; Le choix de la date et du cryptogramme est libre** (Ex : date d'expiration décembre 2010 et CVV =123).

NB : Attention les paiements avec des numéros de cartes réelles en **mode test** passeront en paiement refusé.

Numéro de carte	Cas de test vérifié
Commerçant non enrôlé 3D-Secure	
4970 1000 0000 0003	Paie ment accepté (autorisation accordée)
Commerçant enrôlé 3D-Secure	
4970 1000 0000 0000	Paie ment accepté avec authentification internaute
4970 1000 0000 0001	Paie ment accepté sans authentification internaute (Internaute non enrôlé 3D-Secure)
4970 1000 0000 0002	contacter l'émetteur de carte (Transaction à forcer). Authentification réalisée avec succès.
4970 1000 0000 0006	Problème technique lors du calcul de la garantie de paiement Le paiement est accepté, mais le calcul de la garantie de paiement est impossible (la garantie de paiement est restituée par la plateforme à UNKNOWN)
4970 1000 0000 0007	Problème technique lors de l'authentification porteur Le paiement est accepté, mais la transaction est non garantie (la garantie de paiement est restituée à NO).
4970 1000 0000 0097	Paie ment refusé pour cause d'authentification 3D-Secure échouée (l'internaute n'est pas parvenu à s'authentifier)
4970 1000 0000 0099	Paie ment refusé (autorisation refusée suite à erreur dans le cryptogramme visuel saisi)
4970 1000 0000 0098	Paie ment refusé (autorisation refusée pour cause de plafond dépassé)
4970 1099 9999 9999	Paie ment accepté (utilisation d'une carte étrangère)

Toutes les transactions réalisées en test sont consultables par les personnes habilitées sur le back office Payzen à l'adresse suivante :

<https://secure.payzen.eu/vads-merchant/>

Ces transactions sont disponibles en visualisation via le menu « **Gestion TEST** » situé en haut à droite sur le back office.

Elles sont aussi en visualisation via le menu Gestion (en haut à gauche) en sélectionnant « Transactions Test ».

REMARQUE :

Dans la phase de test, après avoir renseigné dans le back office Payzen, l'URL serveur en mode test, vérifier que sans cliquer sur « retour à la boutique » après paiement, le back office de votre site est correctement renseigné sur l'état du paiement.

4.4. Transmission du PV de recette

Suite à la réalisation des tests, le procès verbal de recette doit être complété et adressé à support@payzen.eu, 72 heures avant la date de mise en production souhaitée.

NB : Les mises en production sont réalisées les jours ouvrés, du lundi au vendredi (heure légale française).

4.5. Activation de la boutique en production

Suite à la validation du PV de recette, votre certificat de production a été généré. Cette génération de certificat est confirmée par un mail transmis au commerçant.

Après réception de cette confirmation, le webmaster doit récupérer le **certificat de production** et modifier la variable **ctx_mode** comme indiqué au paragraphe suivant pour basculer réellement la boutique en production.

4.5.1. Récupération du certificat de production et modification du champ « ctx_mode »

Le certificat de production est alors mis à disposition dans le back office Payzen à l'emplacement suivant : Menu « **Paramétrage** » / **Boutique** / onglet « **Certificat** ». Il vient remplacer celui préalablement fourni dans le cadre des tests.

Il est accessible par toutes les personnes dûment habilitées à cet effet. Pour des raisons de sécurité, **ce certificat ne sera plus consultable dès lors qu'une première transaction (hors paiement manuel) aura été réalisée sur la boutique.**

A ce titre, nous vous demandons de prendre toutes les dispositions sécuritaires appropriées quant à son utilisation et à sa conservation.

La variable ctx_mode doit quant-à-elle désormais être valorisée à PRODUCTION dans votre formulaire.

4.5.2. Réalisation d'une première transaction en production

Il est conseillé au commerçant d'effectuer une transaction afin de vérifier le fonctionnement de bout-en-bout en environnement de production. Cette transaction sera débitée.

Le back office Payzen reste accessible à l'adresse suivante :

<https://secure.payzen.eu/vads-merchant/>

Les transactions sont désormais consultables en visualisation via le menu « **Gestion** », situé en haut à gauche sur l'outil de gestion de caisse.

Vérifier le bon fonctionnement de l'url serveur renseignée le back office, sans cliquer sur le bouton « retour à la boutique ».

5. ASSISTANCE TECHNIQUE

Pour tout problème d'accès à le back office Payzen, il convient d'utiliser les liens « compte bloqué » ou « mot de passe oublié » disponible sur la page de connexion de le back office Payzen.

Pour toute question technique, vous pouvez nous contacter par téléphone au



Accessible les jours ouvrés du lundi au vendredi de 09h00 à 18h00 (heure légale française).

(Tarification de ce numéro: Coût d'un appel local depuis un poste fixe)

6.Acronymes et glossaire

6.1. Acronymes

Acronyme	Signification
3DS	3D-Secure
HTTP	Hypertext Transfer Protocol
MPI	Merchant Plug-in
PCI-DSS	Payment Card Industry Data Security Standard
SHA	Secure Hash Algorithm
URL	Uniform Resource Locator
VAD	Vente A Distance

6.2. Glossaire

Terme	Signification
3D-Secure	Protocole interbancaire permettant d'offrir un niveau de sécurité supplémentaire pour les transactions e-commerce réalisées on-line. Il consiste à demander à l'internaute, en plus de son numéro de carte bancaire et du cryptogramme visuel, une information indépendante de la carte et uniquement connue de lui. Cette authentification supplémentaire permet a priori de s'assurer que la personne qui est en train de réaliser la transaction est le véritable porteur de la carte bancaire.
Acquéreur	Banque ou organisme ayant un contrat avec le commerçant pour la remise en banque de ses paiements.
Authentification	Processus de vérification de l'identité du titulaire de la carte (basé sur le protocole 3D-Secure).
Autorisation	Dans le cadre d'une transaction par carte de paiement, l'autorisation prend effet lorsqu'un commerçant reçoit la permission d'utiliser une carte de paiement pour une transaction particulière.
Boutique	Enseigne commerciale d'un marchand
Canal de vente	Modalité de commercialisation d'un bien ou service par un commerçant (exemple : e-commerce, Serveur vocal, téléphone, e-mail, etc.)
Client	Titulaire d'une carte achetant un bien ou un service chez un commerçant
Commerçant	Marchand vendant des biens ou services
Contrat commerçant	Contrat entre le commerçant et un acquéreur, sur lequel les transactions de paiement sont remises en banque.
Contribution	Module réalisant automatiquement l'interfaçage entre la plateforme de paiement et un logiciel de création de boutique en ligne open-source.
Contrôles locaux	Contrôles internes effectués sur la plateforme de paiement, avant demande d'autorisation, pour lutter contre la fraude.

Terme	Signification
Cryptogramme visuel	Le cryptogramme visuel de la carte correspond au code de 3 chiffres présent au verso des cartes CB, VISA ou MASTERCARD, à droite dans la zone de signature ; ou aux 4 chiffres présents au recto des cartes AMEX. Il permet d'apporter à la transaction un niveau de sécurité supplémentaire.
Demande d'autorisation	Demande effectuée auprès de l'émetteur de la carte pour s'assurer de la validité de la carte du client
E-commerce	Désigne la vente de biens et de services via internet
Emetteur	Banque ou organisme ayant émis la carte du client
Empreinte	Demande d'autorisation de montant inférieur à 2 euros effectuée auprès de l'émetteur pour s'assurer de la validité de la carte.
Enrôlement	Inscription du commerçant ou de son client au service 3D-secure
Favicon	Icône favori de la boutique apparaissant sur l'outil de gestion de caisse
Hachage	Processus qui consiste à rendre des données illisibles en les convertissant en une empreinte numérique de longueur fixe via un algorithme de chiffrement (SHA-1)
http	Protocole Internet ouvert pour le transfert ou la transmission d'informations sur le Web.
Identifiant de site	Identifiant unique attribué par la plateforme de paiement à chaque boutique lors de son inscription
Internaute	Acheteur sur la boutique du e-commerçant
Journal	Reporting pré-formaté restitué au commerçant sous forme fichier
Marchand	Cf. commerçant
Merchant Plug-in	Module utilisé dans le traitement des authentifications 3D-secure. En standard, la plateforme de paiement inclut un merchant plug-in.
Outil de gestion de caisse	Application internet mise à la disposition des commerçants pour paramétrer leur boutique et gérer leurs transactions
Paiement unitaire	Paiement dont la totalité du montant est débité au porteur de carte en une seule fois
Paiement en plusieurs fois / paiement en n fois	Paiement débité en plusieurs échéances au porteur de carte (et crédits en plusieurs échéance au commerçant)
Porteur de carte	Client du commerçant titulaire de la carte utilisée
PCI-DSS	Norme sécuritaire développée dans le but de renforcer la sécurité des données des titulaires de cartes et de faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale.
Plateforme de paiement	Serveur de paiement sécurisé
Présentation en banque	Transmission des paiements à l'acquéreur pour débiter le porteur et créditer le compte du commerçant.
Procès verbal de recette	Document devant impérativement être renseigné et retourné pour permettre le passage en production de la boutique

Terme	Signification
Query string	Partie de l'URL contenant les paramètres de retour exploitables par le commerçant. https://server/path/program?query_string
Remise en banque	Cf Présentation en banque
SHA-1	Algorithme de chiffrement irréversible (Secure Hash Algorithm)
Signature	Donnée permettant d'authentifier l'expéditeur d'un message
Site	Cf. Boutique
Systempay	Nom de la plateforme de paiement sécurisée
Type de carte	Réseau d'émission de la carte
URL	Adresse web
Validation	Fait d'autoriser l'envoi en banque d'une transaction à la date de présentation demandée
Validation automatique	Présentation automatique des transactions en banque par la plateforme de paiement à la date de présentation demandée sans intervention complémentaire du commerçant.
Validation manuelle	Le commerçant doit impérativement valider manuellement chaque paiement avec son outil de gestion de caisse ou via webservice pour qu'il soit remis en banque à la date de présentation demandée. Cette action ne peut être réalisée que jusqu'au jour de la date de présentation demandée.
Vente à distance	Paiement initié depuis tout autre canal de vente que le e-commerce Il peut s'agir d'une saisie manuelle, d'un paiement initié via un Serveur Vocal Interactif, etc.

7. ANNEXES

7.1. Exemples d'implémentation

7.1.1. CONTROLE DE LA SIGNATURE (Java)

L'algorithme SHA1 est disponible dans la plupart des langages utilisés dans le développement d'applications Web. Voici un exemple de vérification de signature en Java, dans un environnement JSP / Servlet, avec le framework *Struts* :

Tout d'abord, créons une classe utilitaire Sha, qui contiendra ce qui est nécessaire au traitement de l'algorithme SHA1 :

```
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("iso-8859-1");

            md.update(bytes, 0, bytes.length);
            byte[] shalhash = md.digest();

            return convertToHex(shalhash);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

    private static String convertToHex(byte[] shalhash) {
        StringBuilder builder = new StringBuilder();
        for (int i = 0; i < shalhash.length; i++) {
            byte c = shalhash[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));
    }
}
```

```
}
```

Ensuite, voici le traitement de vérification lui-même :

```
@ActionMethod("return")
public ActionForward performCheck(ActionMapping actionMapping,
    OrderForm form, HttpServletRequest request,
    HttpServletResponse response) {

    String fields[] = {
        "version",      "site_id",      "ctx_mode",      "trans_id",      "trans_date",
        "validation_mode", "capture_delay", "payment_config", "card_brand",
        "card_number",    "amount",    "currency",    "auth_mode",    "auth_result",
        "auth_number", "warranty_result", "payment_certificate", "result" };

    StringBuilder builder = new StringBuilder();
    for (String field : fields) {
        String value = request.getParameter(field);
        builder.append(value);
        builder.append(Sha.SEPARATOR);
    }
    builder.append(key);

    String c_sign = Sha.encode(builder.toString());
    if (c_sign.equals(request.getParameter("signature"))) {
        return new ActionForward("/ok.jsp");
    } else {
        return new ActionForward("/fail.jsp");
    }
}
```


7.1.2. Acquisition des données carte déléguées à la plateforme (PHP)

Cet exemple de code affiche un simple bouton « Payer », qui soumet un formulaire tel que l'attend la plateforme.

L'acquisition des données carte est donc réalisée par la plateforme.

```
<?php
$key = "votre certificat personnel, à récupérer dans le back-office";

// Initialisation des paramètres
$params = array(); // tableau des paramètres du formulaire

$params['vads_site_id'] = "votre identifiant boutique";

$montant_en_euro = 9.99;
$params['vads_amount'] = 100*$montant_en_euro; // en cents
$params['vads_currency'] = "978"; // norme ISO 4217
$params['vads_ctx_mode'] = "TEST";
$params['vads_page_action'] = "PAYMENT";
$params['vads_action_mode'] = "INTERACTIVE"; // saisie de carte
réalisée par la plateforme
$params['vads_payment_config'] = "SINGLE";
$params['vads_version'] = "V2";

// Exemple de génération de trans_id basé sur l'horodatage
$ts = time();
$params['vads_trans_date'] = date("YmdHis", $ts);
$params['vads_trans_id'] = date("His", $ts);

// Génération de la signature
ksort($params); // tri des paramètres par ordre alphabétique
$contentu_signature = "";
foreach ($params as $nom => $valeur)
{
    $contentu_signature .= $valeur."+";
}
$contentu_signature .= $key; // On ajoute le certificat à la fin
$params['signature'] = sha1($contentu_signature);
?>
<html>
<head>
<title>Redirection vers la plateforme de paiement</title>
</head>
<body>
<form method="POST" action="https://secure.payzen.eu/vads-payment/">
<?php
foreach($params as $nom => $valeur)
{
    echo '<input type="hidden" name="' . $nom . '" value="' .
    $valeur . '" />';
}
?>
<input type="submit" name="payer" value="Payer" />
</form>
</body>
</html>
```

7.1.3. Acquisition des données carte par le commerçant (PHP)

Cet exemple implémente un formulaire de saisie de carte minimaliste, avec la génération du formulaire à destination de la plateforme.

Tout d'abord, voici le formulaire de saisie proprement dit :

```
<html>
<head>
<title>Saisissez les informations de votre carte</title>
</head>
<body>
<form action="3DS_form_paiement.php" method="POST">
  <fieldset>
    <legend>Formulaire de paiement par CB</legend>

    <label for="vads_card_number">Numéro de carte</label><br/>
    <input type="text" name="vads_card_number" size="19"/>
    <br/>
    <label>Date d'expiration</label><br/>
    <input type="text" name="vads_expiry_month" size="2"/> / <input
type="text" name="vads_expiry_year" size="4"/>
    <br/>
    <label for="vads_cvv">Cryptogramme</label><br/>
    <input type="text" name="vads_cvv" size="3"/>
    <br/>
    <input type="submit" value="Payer"/>
  </fieldset>
</form>
</body>
</html>
```

Ce formulaire poste les informations de carte vers une page nommée « 3DS_form_paiement.php » qui va être chargée de générer le formulaire à destination de la plateforme.

En voici le code :

```
<?php
$key = "votre certificat personnel, à récupérer dans le back-office";

// Initialisation des paramètres
$params = array(); // tableau des paramètres du formulaire

$params['vads_site_id'] = "votre identifiant boutique";

$montant_en_euro = 9.99;
$params['vads_amount'] = 100*$montant_en_euro; // en cents
$params['vads_currency'] = "978"; // norme ISO 4217
$params['vads_ctx_mode'] = "TEST";
$params['vads_page_action'] = "PAYMENT";
$params['vads_action_mode'] = "SILENT"; // saisie de carte réalisée par le site marchand
$params['vads_payment_config'] = "SINGLE";
$params['vads_version'] = "V2";

// Exemple de génération de trans_id basé sur l'horodatage
$ts = time();
$params['vads_trans_date'] = date("YmdHis", $ts);
$params['vads_trans_id'] = date("His", $ts);
```

```
// Paramètres liés à la carte bancaire du client
$champs_carte
array('vads_card_number', 'vads_expiry_month', 'vads_expiry_year', 'vads_cvv');
foreach ($champs_carte as $champ_carte)
{
    $params[$champ_carte] = $_POST[$champ_carte];
}
$params['vads_payment_cards'] = "CB"; // préciser le type de carte qui a été
utilisée

// Génération de la signature
ksort($params); // tri des paramètres par ordre alphabétique
$contenu_signature = "";
foreach ($params as $nom => $valeur)
{
    $contenu_signature .= $valeur."+";
}
$contenu_signature .= $key; // On ajoute le certificat à la fin
$params['signature'] = sha1($contenu_signature);
?>
<html>
<head>
    <title>Redirection vers la plateforme de paiement</title>
</head>
<!-- On fait soumettre le formulaire immédiatement par javascript -->
<body onload="document.forms[0].submit();">
<form method="POST" action="https://secure.payzen.eu/vads-payment/">
<?php
foreach($params as $nom => $valeur)
{
    echo '<input type="hidden" name="' . $nom . '" value="' . $valeur . '" />';
}
?>
</form>
</body>
</html>
```

Ici, la redirection est effectuée immédiatement en javascript.

7.1.4. Acquisition des données carte par le commerçant (PHP)

Cet exemple montre comment procéder pour vérifier ce qui est transmis par la plateforme en retour, que ce soit par l'URL serveur, ou par redirection suite à un « retour boutique » effectué à l'initiative du client :

```

<?php
$key = "votre certificat personnel, à récupérer dans le back-office";

$contentu_signature = "";
$params = $_POST;
ksort($params);
foreach ($params as $nom => $valeur)
{
    if(substr($nom,0,5) == 'vads_')
    {
        // C'est un champ utilisé pour calculer la signature
        $contentu_signature .= $valeur."+";
    }
}
$contentu_signature .= $key; // On ajoute le certificat (dernier paramètre)
$signature_calculée = sha1($contentu_signature);

if(isset($_POST['signature']) && $signature_calculée == $_POST['signature'])
{
    // Requête authentifiée
    // Attention cependant à bien vérifier les paramètres passés
    // Notamment le vads_site_id et le vads_ctx_mode

    if($_POST['vads_result'] == "00")
    {
        // Paiement ok
    }
    else
    {
        // Paiement refusé ou referral
    }
}

```

Ici, la redirection est effectuée immédiatement en javascript.

7.2. Pages standards de la plateforme de paiement

Ces pages sont spécifiques aux commerçants déléguant l'acquisition des données carte à la plateforme de paiement.

Les textes et visuels ci-dessous ne sont pas contractuels.

Sélection du type de carte :

The screenshot displays the PAYZEN payment interface. At the top left is the PAYZEN logo. Below it is a placeholder for the merchant's logo, labeled "Logo de votre boutique", featuring a colorful graphic of a laptop and abstract shapes. A green header bar contains the text "INFORMATION SUR LA TRANSACTION". Below this, the text "URL Boutique" is followed by transaction details: "Identifiant du commerçant : 95343937", "Numéro de transaction : 984486", and "Montant : 100,00 EUR". Another green header bar contains the text "CHOISISSEZ VOTRE MOYEN DE PAIEMENT". Below this, the text "Choisissez votre moyen de paiement :" is followed by a row of payment method icons: VISA, Mastercard, American Express, and others. Below the icons are two buttons: "Valider la commande." and "Annuler et retourner à la boutique". At the bottom left is the PCI DSS logo, and at the bottom right is the YRA logo. A small copyright notice "copyright©2009, tous droits réservés" is visible near the bottom right.

Saisie des informations de la carte :



The image shows a web-based payment interface for PayZen. At the top left is the PayZen logo. Below it is a colorful graphic of a laptop with a shopping bag and the text "Logo de votre boutique". To the right is the "Verified by VISA" logo. The main content area is divided into two sections: "Informations sur la transaction" and "Paiement sécurisé". The first section displays transaction details: merchant ID (65201958), transaction number (756700), and amount (331,60 EUR). The second section explains security symbols and provides input fields for the card number, expiration date (month and year), and a visual cryptogram. A green "Validier" button is positioned below the cryptogram field. At the bottom right, there is a button to "Annuler et retourner à la boutique". The footer includes PCI DSS and YRA logos, along with a copyright notice for PayZen © 2010.

PAYZEN

Logo de votre boutique

Verified by VISA

Informations sur la transaction

Identifiant du commerçant : 65201958
Numéro de transaction : 756700
Montant : 331,60 EUR

Paiement sécurisé

Les symboles   indiquent que vous êtes sur un site sécurisé et que vous pouvez régler votre achat en toute tranquillité.

Numéro de carte : Expire fin :

Cryptogramme visuel de la carte : 

> Validier

> Annuler et retourner à la boutique

Copyright PayZen © 2010, tous droits réservés

PCI DSS **YRA**

Compte rendu d'une transaction réussie



Votre demande de paiement a été enregistrée avec succès.

Détail du paiement



Identifiant du commerçant : 95343937
Numéro de transaction : 984486
Date/ Heure : 9/12/2009 / 16:41
Moyen de paiement : MASTERCARD
Numéro de carte : 419310XXXXXX0008 04/10
Montant : 100,00 EUR
Numéro d'autorisation : 014786
Certificat 3D Secure :
Certificat : 56469340936365749R456h78436234o758347S5897V?N39587120

[Retourner à la boutique](#)

copyright©2009, tous droits réservés



Message d'échec de transaction




Votre demande de paiement a été refusée par votre établissement.

Détail du paiement

Identifiant du commerçant : 95343937
Numéro de transaction : 984486
Date/ Heure : 9/12/2009 / 16:41
Moyen de paiement : MASTERCARD
Numéro de carte : 419310XXXXXX0008 04/10
Montant : 100,00 EUR
Numéro d'autorisation : 014786
Certificat 3D Secure :
Certificat : 56469340936365749R456h78436234o758347S5897V?N39587120

[Annuler](#)

copyright©2009, tous droits réservés



7.3. Personnalisation des pages de paiement à l'aide du paramètre « vads_theme_config ».

7.3.1. Principe de fonctionnement

Dans le formulaire envoyé à l'URL de paiement, il est possible de spécifier un paramètre nommé **vads_theme_config** afin de personnaliser l'affichage des pages de paiement.

Ce paramètre contient une liste de mots-clés (codes) associés à des éléments des pages de paiement (libellés, images), auxquels on associe une valeur. Le formalisme du paramètre est le suivant :

Code1=Valeur1 ;Code2=Valeur2

Les éléments personnalisables sont les suivants :

Code	Description
SUCCESS_FOOTER_MSG_RETURN	Libellé remplaçant « Retour à la boutique » lors d'un paiement réalisé avec succès.
CANCEL_FOOTER_MSG_RETURN	Libellé remplaçant « Annuler et retourner à la boutique » pendant les phases de sélection puis de saisie de carte, et en cas d'échec du paiement.

7.3.2. Exemple d'utilisation

En renseignant **vads_theme_config** avec la valeur suivante :

SUCCESS_FOOTER_MSG_RETURN=Retour **au**
site;CANCEL_FOOTER_MSG_RETURN=Annuler et retourner au site

La page de saisie de carte bancaire devient alors :

PAYZEN

Logo de votre boutique

Verified by VISA

Informations sur la transaction

Identifiant du commerçant : 65201958
Numéro de transaction : 756700
Montant : 331,60 EUR

Paieement sécurisé

Les symboles indiquent que vous êtes sur un site sécurisé et que vous pouvez régler votre achat en toute tranquillité.

Numéro de carte : Expire fin : mois année

Cryptogramme visuel de la carte :

> Valider

> Annuler et retourner à la boutique

Copyright PayZen © 2010 tous droits réservés

PCI DSS **YRA**

Le libellé « Annuler et retourner à la boutique » a été remplacé par la valeur spécifiée via le code **CANCEL_FOOTER_MSG_RETURN**.

Dans le cas d'un paiement réussi, la page détaillant le paiement devient alors :



Le libellé « Retourner à la boutique » a été remplacé par la valeur spécifiée via le code **SUCCESS_FOOTER_MSG_RETURN**.