

Plateforme Systempay  
Descriptif de l'interface avec la page de paiement

Version 1.11

---



## Rédaction, Vérification, Approbation

Rédaction		Vérification		Approbation	
Nom	Date/Visa	Nom	Date/Visa	Nom	Date/Visa
Lyra-Network	17/12/2008				

## Historique du document

Version	Auteur	Date	Commentaires
1.11	Lyra-Network	23/06/2010	Dans le code php exemple l'identifiant boutique et le certificat sont donné en exemple et ne permette pas de faire un test de paiement. Dans le code est indiqué qu'il faut saisir ses propres valeurs.
1.10	Lyra-Network	21/06/2010	Suppression des limitations des ports possibles pour les URL de retour suite à modification de la plateforme de paiement.
1.9	Lyra-Network	18/06/2010	Modification du code php Ajout commentaire pour l'url serveur
1.8	Lyra-Network	01/03/2010	- Dans la redirection vers la plateforme de paiement, ajout du paramètre contracts - Dans le retour vers le site marchand, ajout du paramètre contract_used
1.7	Lyra-Network	27/01/2010	- Dans la redirection vers la plateforme de paiement, ajout des paramètres contrib, order_info2, order_info3, payment_src ; user_info, theme_config dans la redirection vers la plateforme de paiement - Dans le retour vers le site marchand, ajout des paramètres order_info2, order_info3, payment_src ; user_info, theme_config, language - Ajout de valorisations pour le paramètre extra_result - Modification de la longueur du paramètre order_info
1.6	Lyra-Network	27/01/2010	Complément information sur les ports possible pour les URL de retour ( 80 et 443 ) Complément d'information sur la variable payment_card Ajout code php pour le retour boutique
1.5	Lyra-Network	07/12/2009	Mise à jour de la procédure de téléchargement de logo Acceptation URL de retour serveur les url de type https
1.4	Lyra-Network	26/11/2009	Information complémentaire pour l'URL serveur Information complémentaire pour les paiements de test Information complémentaire pour la variable trans_id
1.3	Lyra-Network	26/10/2009	Modification calcul URL calcul signature URL serveur (positionnement de la valeur hash)
1.2	Lyra-Network	13/10/2009	Ajout rubrique logo Correction EUR par le code monnaie 978 Ajout des paramètres pour calcul signature URL serveur Ajout information sur la définition du trans_id Complément d'information sur URL retour (refus https ) Complément d'information sur le type de carte Correction language japonais ja => jp Ajout contact problème d'accès outils de gestion de caisse

1.1	Lyra-Network	13/05/2009	Ajout du paramètre Extra_result dans le retour vers le site marchand
0.90	Lyra-Network	05/03/2009	Mise à jour avant mise en production.
0.20	Lyra-Network	17/12/2008	Mise en forme, ajout d'un exemple de code.
0.10	Lyra-Network	16/12/2008	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

---

<b>1. PRINCIPE GENERAL .....</b>	<b>1</b>
1.1. Cinématique des échanges .....	1
1.2. Les pages standard de la plateforme de paiement .....	2
1.3. Sécurité .....	3
<b>2. REDIRECTION VERS LA PLATEFORME DE PAIEMENT .....</b>	<b>5</b>
2.1. Format et codage des paramètres .....	5
2.2. Liste des paramètres .....	5
2.3. Signature .....	11
<b>3. RETOUR VERS LE SITE MARCHAND .....</b>	<b>12</b>
3.1. Liste des paramètres .....	13
3.2. Signature .....	17
3.3. Réponse de serveur à serveur .....	17
<b>EXEMPLE DE CONTROLE DE LA SIGNATURE (Java).....</b>	<b>19</b>
<b>4. 19</b>	
<b>5. EXEMPLE D'INTEGRATION (php) .....</b>	<b>21</b>
<b>6. EXEMPLE CONTROLE SIGNATURE (php)- Retour vers boutique .....</b>	<b>23</b>
<b>7. COMMENT ACTIVER LA BOUTIQUE EN PRODUCTION ?....</b>	<b>25</b>
7.1 Phase de test .....	25
7.1.1 Récupération du certificat de test et de l'identifiant du site (site_ID) .....	25
7.1.2 Réalisation des tests .....	25
7.2 Transmission du PV de recette .....	26
7.3 Activation de la boutique en production .....	26
7.3.1 Récupération du certificat de production .....	26
7.3.2 Réalisation d'une première transaction en production .....	27
<b>8. MISE EN PLACE DU LOGO SUR LA PAGE DE PAIEMENT ....</b>	<b>27</b>
<b>9. ASSISTANCE TECHNIQUE .....</b>	<b>27</b>

## 1. PRINCIPE GENERAL


### 1.1. Cinématique des échanges

La cinématique d'échange est la suivante :

- 1) Une fois la commande de l'internaute complète, 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 suivant.
- 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.
- 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 redirection vers un ACS 3D-Secure aura éventuellement lieu, puis une demande d'autorisation sera effectuée auprès de l'acquéreur concerné, 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. Si l'option est active, un e-mail de confirmation de transaction sera envoyé à l'internaute.

## 1.2. Les pages standard de la plateforme de paiement

Sélection du type de carte :



**BANQUE POPULAIRE OCCITANE** Cyberplus Paiement

**Informations sur la transaction**

<https://laboutique.cyberpluspaiement.com>





Identifiant du commerçant : 12345678912345

Référence de la transaction : 123456

Montant de la transaction : 100,00 EUR

**Paiement sécurisé**

Choisissez votre moyen de paiement :



[> Annuler et retourner à la boutique](#)

Copyright © 2009, tous droits réservés

Saisie des informations de la carte :



**BANQUE POPULAIRE OCCITANE** Cyberplus Paiement



**Informations sur la transaction**

<https://laboutique.cyberpluspaiement.com>

Identifiant du commerçant : 12345678912345

Référence de la transaction : 123456

Montant de la transaction : 100,00 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 : Mois  Année

Cryptogramme visuel de la carte :  ?

[> Valider](#)

[> Annuler et retourner à la boutique](#)

Copyright © 2009, tous droits réservés



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://systempay.cyberpluspaiement.com/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.
- **Obligatoire** : indique si la présence du paramètre est obligatoire. *Attention, un paramètre obligatoire peut être vide.*
- **Signature** : indique si ce paramètre est utilisé dans le calcul de la signature.
- **Remarques** : remarques sur l'utilisation de ce paramètre.
- **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.

### 2.2. Liste des paramètres

Nom	Format	Exemple	Obligatoire	Signature	Remarques	Code
amount	n..12	1500	oui	oui		09
capture_delay	n..3	3	oui	oui	vide : valeur configurée par défaut, sinon, nombre de jours	06
contrib	ans..255					31
currency	n3	978	oui	oui	norme ISO 4217 978 pour EURO	10
cust_address	an..255					19
cust_country	a2	FR			norme 3166-1	22
cust_email	an.127					15
cust_id	an..63					16
cust_name	an..127					18

Nom	Format	Exemple	Obligatoire	Signature	Remarques	Code
cust_phone	an..63					23
cust_title	an..63					17
cust_city	an..63					21
cust_zip	an..63					20
ctx_mode		TEST	oui	oui	TEST ou PRODUCTION	11
language	a2	fr			norme ISO 639-1	12
order_id	an..12					13
order_info	an..255					14
order_info2	an..255					14
order_info3	an..255					14
payment_cards	an..127	VISA;MA STERCA RD	oui	oui	Valorisation à vide conseillée « ; »	08
payment_config			oui	oui	SINGLE ou MULTI (avec des paramètres).	07
payment_src	a..5	MOTO			Vide, BO, MOTO, CC ou OTHER	60
signature	an40	7e4cd326 5ce8f475 35a52e19 c4446d2f e4fc8acb	oui			
site_id	n8		oui	oui		02
theme_config	ans..255					32
trans_date	n14	20090323 105432	oui	oui		04
trans_id	n6		oui	oui	Compris entre 000000 et 899999	03
validation_mode	n..1		oui	oui	vide : valeur configurée par défaut 0 : validation automatique 1 : validation manuelle	05
version		V1	oui	oui		01
url_success	ans..127					24
url_referral	ans..127					26
url_refused	ans..127					25
url_cancel	ans..127					27
url_error	ans..127					29
url_return	ans..127					28
user_info	ans..255					61
contracts	ans..255					62

### amount

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

### capture\_delay

Descriptif de l'interface vers la page de paiement  
©Lyra Network- 6/27

Paramètre **obligatoire** indiquant le délai en nombre de jours avant remise en banque. Si ce paramètre est vide (il doit néanmoins être transmis), alors la valeur par défaut sera utilisée. Cette dernière est paramétrable dans l'outil de gestion de caisse Cyberplus Paiement par toutes les personnes dûment habilitées.

### contracts

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

RESEAU1=contratReseau1;RESEAU2=contratReseau2;RESEAU3=contratReseau3

Les différents réseaux étant :

Réseau	Valorisation 'contracts'
American Express	AMEX
CB	CB

### contrib

Information complémentaire facultative destinée à indiquer le nom de la contribution utilisée lors du paiement (joomla, oscommerce...).

### 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](http://www.iso.org/iso/support/currency_codes_list-1.htm)

Pour l'Euro, la valeur est 978.

### cust\_email

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

### cust\_id

Paramètre facultatif correspondant à un identifiant client pour le marchand.

### cust\_name, cust\_title, cust\_address, cust\_zip, cust\_city, cust\_phone

Paramètres optionnels concernant le client, et correspondant respectivement à :

- cust\_name : nom du client
- cust\_title : civilité du client
- cust\_address : adresse du client
- cust\_zip : code postal du client
- cust\_city : ville du client
- cust\_phone : numéro de téléphone du client

### cust\_country

Code pays du client à la norme ISO 3166. Paramètre optionnel.

[http://www.iso.org/iso/english\\_country\\_names\\_and\\_code\\_elements](http://www.iso.org/iso/english_country_names_and_code_elements)

Pour la France, le code est FR.

### 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.

### language

Paramètre optionnel indiquant la langue de 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
<b>Français</b>	<b>fr</b>
Italien	it
Japonais	jp

Par défaut, le français est sélectionné.

### order\_id

Ce paramètre est optionnel. Il correspond à un numéro de commande qui pourra être rappelé dans l'e-mail adressé au client. Sa taille maximale est de 12 caractères alphanumériques.

### order\_info, order\_info2, order\_info3

Ces paramètres optionnels sont des champs libres. Ils peuvent par exemple servir à stocker un résumé de la commande.

### payment\_cards

Ce paramètre **obligatoire** contient la liste des types de cartes disponibles pour ce site, 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 types de carte 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

### 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 :

currency=978

amount=10000

payment\_config=**MULTI:first=5000;count=3;period=30**

Dans cette configuration :

- Un premier paiement de 50 euros sera effectué à aujourd'hui + « capture\_delay » jours.
- Un deuxième paiement de 25 euros sera effectué à aujourd'hui + « capture\_delay » + 30 jours.
- Un troisième et dernier paiement de 25 euros sera effectué à aujourd'hui + « capture\_delay » + 60 jours.

*Remarque : si la date de validité de la carte ne permet pas de réaliser le dernier paiement, la demande sera refusée par la plateforme.*

### payment\_src

Paramètre facultatif définissant la source du paiement :

- **Paramètre non défini ou valeur vide**, indique un paiement de type eCommerce. Dans ce cas, la garantie de paiement est calculée conformément aux options du commerce concerné.
- **BO** indique un paiement effectué depuis le « Back Office » (saisie manuelle), dans ce cas il n'y a pas de garantie de paiement.
- **MOTO** indique un paiement effectué par un opérateur suite à une commande par téléphone ou eMail (Mail Or Telephone Order).
- **CC** indique un paiement effectué via un centre d'appel (Call Center).
- **OTHER** indique un paiement effectué par toute autre source que celles précédemment définies.

Des informations complémentaires sur l'origine du paiement peuvent être définies dans le paramètre **user\_info**.

NB : L'utilisation de ce paramétrage n'est permise que pour les commerçants ayant souscrit une offre adéquate. Merci de contacter votre chargé de clientèle bancaire pour plus d'informations.

### signature

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

**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 Cyberplus Paiement dans l'onglet « Paramétrages » / « Boutique » par toutes les personnes habilitées.

**theme\_config**

Paramètre facultatif permettant de personnaliser certains paramètres de la page de paiement standard, comme les logos, bandeaux et certains messages. Contacter le support technique ([supportvad@lyra-network.com](mailto:supportvad@lyra-network.com)) pour plus d'informations.

**trans\_date**

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

**trans\_id**

Ce paramètre est **obligatoire**. Il est constitué de 6 caractères numériques et doit être unique pour chaque transaction sur un site donné sur la journée. En effet l'identifiant unique de transaction au niveau de la plateforme de paiement est constitué du **site\_id**, de **trans\_date** restreint à la valeur de la journée (partie correspondant à AAAAMMJJ) et de **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**.

**validation\_mode**

Paramètre **obligatoire** indiquant si cette transaction devra faire l'objet d'une validation manuelle de la part du commerçant. Si ce paramètre est vide alors la configuration par défaut du site sera prise. Cette dernière est paramétrable dans l'outil de gestion de caisse Cyberplus Paiement par toutes les personnes dûment habilitées.

**version**

Paramètre **obligatoire**. La version actuelle est **V1**.

**url\_success**

URL facultative où sera redirigé le client en cas de succès du paiement, après appui du bouton " retourner à la boutique ".

**url\_referral**

URL facultative où sera redirigé le client en cas de refus d'autorisation avec le code 02 « referral », après appui du bouton " retourner à la boutique ".

**url\_refused**

URL facultative où sera redirigé le client en cas de refus pour toute autre cause que le " referral ", après appui du bouton " retourner à la boutique ".

**url\_cancel**

URL facultative où sera redirigé le client si celui-ci appuie sur " annuler et retourner à la boutique " avant d'avoir procédé au paiement.

#### **url\_error**

URL facultative où sera redirigé le client en cas d'erreur de traitement interne.

#### **url\_return**

URL facultative 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).

#### **user\_info**

Paramètre facultatif spécifiant des informations complémentaires quant au paiement. Dans le cas d'un paiement via une saisie manuelle, ce paramètre contient l'identifiant de l'utilisateur à l'origine de la transaction. Dans les autres cas de paiement (eMail, téléphone...) tels que définis par le paramètre **payment\_src**, ce paramètre doit servir à identifier l'opérateur à l'origine de la transaction.

### **2.3. Signature**

La signature sera constituée des champs suivants :

- version
- site\_id
- ctx\_mode
- trans\_id
- trans\_date
- validation\_mode
- capture\_delay
- payment\_config
- payment\_cards
- amount
- currency
- Valeur du certificat en fonction du mode

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

**L'ordre des champs doit respecter la liste ci-dessus.**

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 :

- version = V1
- site\_id = 12345678
- ctx\_mode = TEST
- trans\_id = 654321
- trans\_date = 20090501193530
- validation\_mode = 1
- capture\_delay = 3
- payment\_config = SINGLE
- payment\_cards = VISA;MASTERCARD
- amount = 1524
- currency = 978
- Valeur du certificat en fonction du mode = 1122334455667788

Et que la valeur du certificat de test est 1122334455667788, alors la chaîne à utiliser pour le hachage à l'aide de l'algorithme SHA1 sera la suivante :

V1+12345678+TEST+654321+20090501193530+1+3+SINGLE+VISA;MASTERCARD+1524+978+1122334455667788

### **3. RETOUR VERS LE SITE MARCHAND**

Cette redirection est effectuée via un formulaire HTTP POST. 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.

Les champs optionnels de la requête sont renvoyés tels quels dans la réponse, mais ne font pas partie de la signature. **Il est recommandé de ne pas faire dépendre un traitement critique de la valeur de ceux-ci.**

### 3.1. Liste des paramètres

Nom	Format	Obligatoire	Signature	Remarques
amount		oui	oui	idem requête
auth_result	n2	oui	oui	vide si erreur avant autorisation
auth_mode		oui	oui	MARK : prise d'empreinte FULL : autorisation du montant total (ou du montant initial dans le cas du paiement en N fois)
auth_number	n6	oui	oui	vide si autorisation échouée.
capture_delay	n..3	oui	oui	valeur par défaut ou valeur spécifiée dans requête
card_brand	an..127	oui	oui	vide si aucune carte n'a été sélectionnée (retour à la boutique).
card_number	an..19	oui	oui	numéro masqué
ctx_mode		oui	oui	idem requête
currency		oui	oui	idem requête
extra_result	n2	oui		numérique, peut être vide.
payment_config		oui	oui	idem requête
Signature		oui		
site_id		oui	oui	idem requête
trans_date		oui	oui	idem requête
trans_id		oui	oui	idem requête
validation_mode	n1	oui	oui	valeur par défaut ou valeur spécifiée dans la requête
warranty_result		oui	oui	vide ou YES, NO, UNKNOWN
payment_certificate	an40	oui	oui	vide si paiement échoué
result	n2	oui	oui	numérique, toujours renseigné
version		oui	oui	Idem requête
order_id				Idem requête
order_info				Idem requête
order_info2				Idem requête
order_info3				Idem requête
cust_address				Idem requête
cust_country				Idem requête
cust_email				Idem requête
cust_id				Idem requête
cust_name				Idem requête
cust_phone				Idem requête
cust_title				Idem requête
cust_city				Idem requête
cust_zip				Idem requête
language				valeur par défaut ou valeur spécifiée dans requête

Nom	Format	Obligatoire	Signature	Remarques
payment_src				Idem requête
user_info				Idem requête
theme_config				Idem requête
contract_used	ans..255			Contrat utilisé

**amount, currency, payment\_config, site\_id, trans\_date, trans\_id, version, payment\_src, user\_info, theme\_config, order\_info, order\_info2, order\_info3, cust\_address, cust\_country, cust\_email, cust\_id, cust\_name, cust\_phone, cust\_title, cust\_city, cust\_zip**

Mêmes valeur que la requête.

#### 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

#### auth\_number

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

### **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.

### **capture\_delay**

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

### **card\_brand**

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

### **card\_number**

Numéro de carte masqué.

### **contract\_used**

Ce paramètre n'est disponible en retour que dans le cas où le paramètre « contracts » a été valorisé dans la requête.

Il contient le réseau et le contrat qui ont effectivement été utilisés pour réaliser la demande d'autorisation.

Le formalisme du paramètre est le suivant :

RESEAU=contratReseau

Les différents réseaux étant :

Réseau	Valorisation 'contracts'
American Express	AMEX
CB	CB

### **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).

### **validation\_mode**

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

### 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

### 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.**

### 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 **extra\_result**.
- 96 : Erreur technique lors du paiement.

### extra\_result

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

Lorsque **result** vaut 30 (erreur de requête), alors 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 **result** vaut 05 (refusée) ou 00 (acceptée), alors 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

### 3.2. Signature

Pour les URL de retour passées en paramètre, la signature sera constituée des champs suivants :

- 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
- Valeur du certificat en fonction du mode

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.

### 3.3. Réponse de serveur à serveur

Cette option permet de spécifier une **URL sur l'outil de gestion de caisse**, que la plateforme de paiement peut 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 vus précédemment, **plus un paramètre supplémentaire nommé « hash » inclus dans le calcul de la signature**.

**Attention cette URL à renseigner dans l'outil de gestion de caisse, dans l'onglet paramétrage/boutique est fortement conseillé si vous souhaitez que la back office de la boutique soit renseigné dans le cas où le client ne clique pas après le paiement sur retour à la boutique.**

**L'URL serveur peut être rejouée dans le back office, par conséquent il nécessaire que le process appelé par l'url serveur prenne en compte que pour une même commande cette url peut-être appelée plusieurs fois sans générer des désagréments au niveau de la boutique comme la gestion des stocks etc ...**

Le calcul de la signature doit donc être réalisé de la manière suivante :

Paramètre à prendre en compte :

- 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
- **hash**
- Valeur du certificat en fonction du mode

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

## EXEMPLE DE 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 :

```

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");
    }
}

```

Pour la vérification de la requête de serveur à serveur, il suffit de reprendre la même routine, et d'ajouter « **hash** » à la fin du tableau **fields()**.

## 5. EXEMPLE D'INTEGRATION (php)

Voici un exemple minimal d'intégration en php.

```
<?php
// saisir votre certificat
$key = "1234567890123456";
$ctx_mode = "TEST";

$amount = 100;
$capture_delay = "";
$currency = "978";
$payment_cards = "";
$payment_config = "SINGLE";
// Saisir votre identifiant boutique
$site_id = "12345678";

// Exemple de génération de trans_id basé sur l'horodatage
$ts = time();
$trans_date = date("YmdHis", $ts);
$trans_id = date("His", $ts);
$validation_mode = "";
$version = "V1";
$url_return = "http://url.de.retour/retour.php";

$signature_contents = $version . "+" . $site_id . "+" . $ctx_mode . "+"
    . $trans_id . "+" . $trans_date . "+" . $validation_mode . "+"
    . $capture_delay . "+" . $payment_config . "+" . $payment_cards . "+"
    . $amount . "+" . $currency . "+" . $key;
$signature = sha1($signature_contents);
?>
<html>
<head>
</head>
<body>
<form method="POST" action="https://systempay.cyberpluspaiement.com/vads-payment/">
<input type="hidden" name="ctx_mode" value="<?php echo($ctx_mode); ?>" />
<input type="hidden" name="amount" value="<?php echo($amount); ?>" />
<input type="hidden" name="capture_delay" value="<?php echo($capture_delay); ?>" />
<input type="hidden" name="currency" value="<?php echo($currency); ?>" />
<input type="hidden" name="payment_cards" value="<?php echo($payment_cards); ?>" />
<input type="hidden" name="payment_config" value="<?php echo($payment_config); ?>"
/>
<input type="hidden" name="site_id" value="<?php echo($site_id); ?>" />
<input type="hidden" name="trans_date" value="<?php echo($trans_date); ?>" />
<input type="hidden" name="trans_id" value="<?php echo($trans_id); ?>" />
<input type="hidden" name="validation_mode" value="<?php echo($validation_mode);
?>" />
<input type="hidden" name="version" value="<?php echo($version); ?>" />
<input type="hidden" name="url_return" value="<?php echo($url_return); ?>" />
<input type="hidden" name="signature" value="<?php echo($signature); ?>" />
<input type="submit" name="payer" value="Payer" />
</form>
</body>
</html>
```

Le formulaire résultant est le suivant :

```
<html>
<head>
</head>
<body>
<form method="POST" action="https://systempay.cyberpluspaiement.com/vads-payment/">
<input type="hidden" name="ctx_mode" value="TEST" />
<input type="hidden" name="amount" value="100" />
<input type="hidden" name="capture_delay" value="" />
<input type="hidden" name="currency" value="978" />
<input type="hidden" name="payment_cards" value="VISA;MASTERCARD" />
<input type="hidden" name="payment_config" value="SINGLE" />
<input type="hidden" name="site_id" value="91485686" />
<input type="hidden" name="trans_date" value="20090324122302" />
<input type="hidden" name="trans_id" value="122302" />
<input type="hidden" name="validation_mode" value="" />
<input type="hidden" name="version" value="V1" />
<input type="hidden" name="url_return" value="http://url.de.retour/retour.php" />
<input type="hidden" name="signature"
value="a492d355c3d81012f12cca86beb8698d1e42bf3f" />
<input type="submit" name="payer" value="Payer" />
</form>
</body>
</html>
```

## 6. EXEMPLE CONTROLE SIGNATURE (php)- Retour vers boutique

Lors du retour vers la boutique par le bouton retour à la boutique ou par l'URL serveur il est conseillé de vérifier la signature présente dans le message de retour.

Veuillez trouver ci-après un code minimal en php

```
<?php
// valeur du certificat.
// Ici cette valeur est ecrite en dur mais vous devez la lire depuis votre base de
données
$key="0494832677774665";

//-----

//Calcul de la signature pour ensuite la vérifier avec celle reçue
//-----

//vérification reception variable hash
// hash reçu => alors reception depuis URL Serveur ( auto réponse )
// Attention vous devez renseigner l'URL serveur dans l'outil de gestion de caisse.

if (isset($_POST['hash'])) {

    $chaine=$_POST['version'] . "+" . $_POST['site_id'] . "+" .
$_POST['ctx_mode'] . "+"
. $_POST['trans_id'] . "+" . $_POST['trans_date'] . "+" . $_POST['validation_mode']
. "+"
. $_POST['capture_delay'] . "+" . $_POST['payment_config'] . "+" .
$_POST['card_brand'] . "+" . $_POST['card_number'] . "+"
. $_POST['amount'] . "+" . $_POST['currency'] . "+" . $_POST['auth_mode'] . "+" .
$_POST['auth_result'] . "+" . $_POST['auth_number'] . "+"
. $_POST['warranty_result'] . "+" . $_POST['payment_certificate'] . "+" .
$_POST['result'] . "+" . $_POST['hash'] . "+" . $key;

}

// hash pas reçu => alors reception depuis le click retour à la boutique
else {

    $chaine=$_POST['version'] . "+" . $_POST['site_id'] . "+" .
$_POST['ctx_mode'] . "+"
. $_POST['trans_id'] . "+" . $_POST['trans_date'] . "+" . $_POST['validation_mode']
. "+"
. $_POST['capture_delay'] . "+" . $_POST['payment_config'] . "+" .
$_POST['card_brand'] . "+" . $_POST['card_number'] . "+"
. $_POST['amount'] . "+" . $_POST['currency'] . "+" . $_POST['auth_mode'] . "+" .
$_POST['auth_result'] . "+" . $_POST['auth_number'] . "+"
. $_POST['warranty_result'] . "+" . $_POST['payment_certificate'] . "+" .
$_POST['result'] . "+" . $key;

}
$signature_shop=sha1($chaine);
```

```
//-----  
// comparaison de la signature reçue et celle calculée  
//-----  
-----  
  
if ($_POST['signature']==$signature_shop) {  
  
    // ok traitement de la commande  
    echo "Controle Signature ok - Traitement commande"."<br>";  
    // le paiement est-il accepté?  
    if ($_POST['result']=="00"){  
        echo "paiement ok";  
    }  
    else{  
        echo "paiement refus autorisation";  
    }  
    }  
    }  
else {  
    // nok ne pas traiter la commande risque de fraude  
    echo "Controle signature Nok - risque de fraude";  
    }  
?>
```

## 7. COMMENT ACTIVER LA BOUTIQUE EN PRODUCTION ?

### 7.1 Phase de test

Préalablement au passage en production du site, 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 de la boutique.

#### 7.1.1 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 Cyberplus Paiement à l'emplacement suivant : Paramètres / Boutique / Certificat.

La donnée 'site\_ID' qui a été automatiquement attribuée à votre boutique lors de l'inscription à Cyberplus Paiement est quant à elle disponible dans l'outil de gestion de caisse Cyberplus Paiement à l'emplacement suivant : Paramètres / Boutique / Configuration générale. Cette valeur doit impérativement être utilisée dans le formulaire HTTP POST.

#### 7.1.2 Réalisation des tests

Les demandes de paiement de test adressées via le formulaire HTTP POST doivent contenir la donnée 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 faisant varier le numéro de carte comme indiqué ci-dessous : (Attention les paiements avec des numéros de cartes réelles en mode test passeront en paiement refusé). Le choix de la date et du cryptogramme est libre (Ex : date d'expiration décembre 2010 et CVV = 123 ).

Numéro de carte	Cas de test vérifié
<b>Commerçant non enrôlé 3D-Secure</b>	
4970 1000 0000 0003	Paiement accepté (autorisation accordée)
<b>Commerçant enrôlé 3D-Secure</b>	
4970 1000 0000 0000	Paiement accepté avec authentification internaute
4970 1000 0000 0001	Paiement 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

Numéro de carte	Cas de test vérifié
4970 1000 0000 0007	Problème technique lors de l'authentification porteur
4970 1000 0000 0097	Paiement refusé pour cause d'authentification 3D-Secure échouée (l'internaute n'est pas parvenu à s'authentifier)
4970 1000 0000 0099	Paiement refusé (autorisation refusée suite à erreur dans le cryptogramme visuel saisi)
4970 1000 0000 0098	Paiement refusé (autorisation refusée pour cause de plafond dépassé)

Toutes les transactions réalisées en test sont consultables par les personnes habilitées sur l'outil de gestion de caisse Cyberplus Paiement à l'adresse suivante :

<https://systempay.cyberpluspaiement.com/vads-merchant/>

Ces transactions sont disponibles en visualisation via le menu « **Gestion TEST** » situé en haut à droite sur l'outil de gestion de caisse.

#### **REMARQUE :**

Dans la phase de test, après avoir renseigné dans l'outil de gestion de caisse 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.

### **7.2 Transmission du PV de recette**

Suite à la réalisation des tests, le procès verbal de recette doit être complété et adressé à [cyberplus.paiement@paiements.natixis.fr](mailto:cyberplus.paiement@paiements.natixis.fr), 72 heures avant la date de mise en production souhaitée.

NB : Les mises en production sont réalisées les jours ouvrés, du lundi au vendredi.

### **7.3 Activation de la boutique en production**

Suite à la validation du PV de recette, la boutique est activée en production de 09h00 à 17h00 (heure légale française).

L'outil de gestion de caisse Cyberplus Paiement reste accessible à l'adresse suivante :

<https://systempay.cyberpluspaiement.com/vads-merchant/>

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

#### **7.3.1 Récupération du certificat de production**

Le certificat de production est alors mis à disposition dans l'outil de Gestion de Caisse Cyberplus Paiement 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 aura été réalisée depuis la boutique.

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

### **7.3.2 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.

Nous rappelons que la variable `ctx_mode` doit désormais être valorisée à PRODUCTION.

**Vérifier le bon fonctionnement de l'url serveur renseigné dans l'outil de gestion de caisse.**

## **8. MISE EN PLACE DU LOGO SUR LA PAGE DE PAIEMENT**

Comme décrit dans le paragraphe 1, il est possible de personnaliser la page de paiement avec l'ajout d'un Logo. Pour cela, vous devez uploader le logo de la boutique par l'intermédiaire de l'outil de gestion de caisse (Menu Paramétrage / Boutique / Personnalisation).

Seuls les utilisateurs ayant les droits de paramétrage sur la boutique peuvent réaliser cette procédure.

## **9. ASSISTANCE TECHNIQUE**

Pour tout problème d'accès à l'outil de gestion de caisse (Première connexion, compte bloqué ou mot de passe perdu), vous pouvez envoyer un mail à l'adresse [cyberplus.paiement@paiements.natixis.fr](mailto:cyberplus.paiement@paiements.natixis.fr)

Pour toute question technique, vous pouvez nous contacter par téléphone au **0811 363 364 (Numéro Azur – Coût d'un appel local depuis un poste fixe) les jours ouvrés** du lundi au vendredi de 09h00 à 18h00 (heure légale française).