Advanced e-Commerce

Guide d'intégration technique pour e-Commerce v.5.3.6

1 Introduction

Advanced e-Commerce détaille l'intégration avancée d'e-Commerce sur votre site Web. Le présent document complète le document Basic e-e-Commerce.

Pour la configuration et la fonctionnalité du site d'administration, veuillez vous reporter au Back-Office User Guide.

2 Best Practices

PostFinance a défini une série de *Meilleures Pratiques* afin de garantir une intégration optimale de votre site avec notre plate-forme de paiement, et s'assurer du traitement fluide de vos transactions.

PostFinance conseille ces *Meilleures Pratiques pour* tous les marchands, et particulièrement pour les plus grands marchands prévoyant un nombre moyen de plus de 1.000 transactions par jour, et/ou des pics de 25 transactions par minute.

Dans le cas où vous vous conformez à ces critères, veuillez nous contacter et demander à notre support technique d'analyser si ces *Meilleures Pratiques* ont bien été implémentées, et de vous donner de l'assistance afin d'encore mieux optimiser votre intégration.

De plus, il est recommandé de prévenir PostFinance à l'avance de la date de lancement de votre site e-Commerce et de vos campagnes/promotions spécifiques qui risquent d'affecter le traffic vers votre boutique en ligne afin que nous puissions prévoir du monitoring et s'assurer que tout fonctionne bien.

Ces *Meilleures Pratiques* peuvent être retrouvées au début de chaque chapitre concerné.

3 Environnement de test

Nous vous conseillons de développer votre intégration dans notre environnement de test avant de transférer en environnement de production. Notre environnement de test fonctionne de manière identique à notre environnement de production, à la différence près que nous n'envoyons pas les transactions à l'acquéreur de la carte et que son utilisation est gratuite.

Notre environnement de test vous permet de simuler des paiements, de modifier la configuration de votre compte et d'affiner l'intégration de notre système de paiement sur votre site Web.

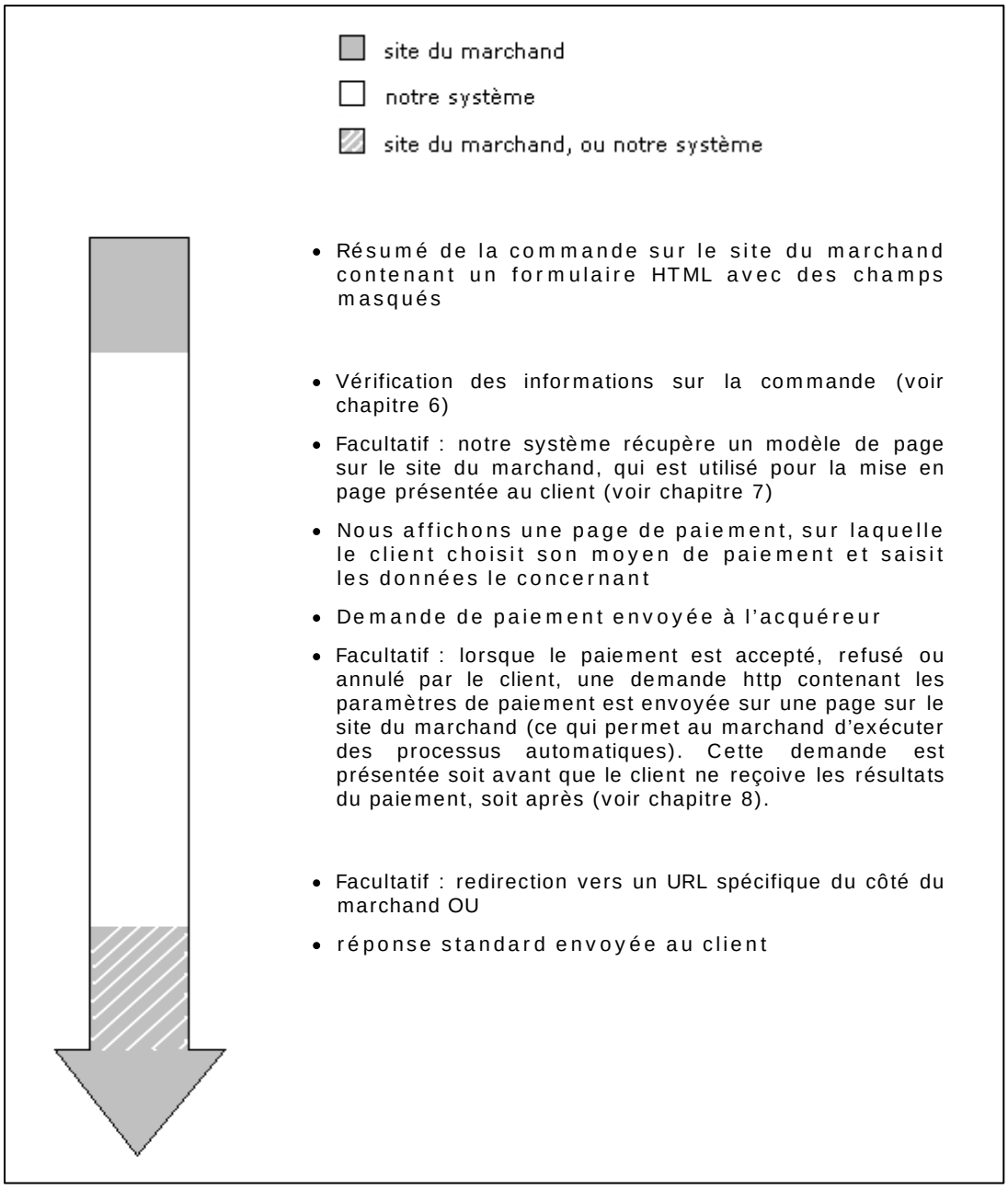
3.1 Configuration de votre compte test.

Lors de votre première connexion à votre compte, vous devrez introduire votre adresse e-mail et changer votre mot de passe. Vous pourrez également introduire/modifier les données techniques de votre compte de test et créer de nouveaux utilisateurs. Pour la création, l'accès et la configuration de votre compte test. Veuillez vous reporter au document Basic e-Commerce. La configuration des informations techniques est expliquée dans les chapitres qui suivent.

Les informations techniques doivent être configurées sur la page d'information technique de votre compte. Vous pouvez accéder aux paramètres techniques par le lien « Information Technique » dans le menu de votre compte.

4 Processus de vente

Le schéma suivant illustre le déroulement des tâches pour une transaction (les étapes obligatoires (en gras) et les étapes facultatives) :



Le marchand peut étendre son intégration en sécurisant les données de commande, en personnalisant les pages de paiement, en demandant des informations au terme d'une transaction et en personnalisant la réponse envoyée à son client.

Le présent manuel explique l'intégration e-Commerce avancé, y compris les étapes facultatives permettant de personnaliser le flux des transactions et d'affiner l'intégration.

Pour une représentation (capture d'écran) d'un processus de vente à la suite d'une intégration e-Commerce de base, veuillez vous reporter au document Basic e-Commerce.

5 Parametres de paiement généraux

Pour certains moyens de paiement (essentiellement les cartes de paiement), les transactions sont réalisées en deux étapes : l'autorisation et la télécollecte (demande de paiement). (Voir chapitres Code d'opération par défaut et Procédure de télécollecte (paiement) par défaut)

Lors de la phase d'autorisation, une demande de réservation du montant de la transaction est effectuée sur la carte du client ; cette demande peut être validée par rapport à une liste noire (opération AUT).

Lors de la phase de télécollecte (demande de paiement), l'acquéreur du marchand est invité à prélever le montant réservé sur la carte du client et à le transférer sur le compte bancaire du marchand (opération DCP).

D'autres moyens de paiement (essentiellement les cartes de paiement) permettent un traitement des transactions en ligne ou hors-ligne. (Voir chapitre Traitement pour les transactions individuelles)

Le marchand peut charger notre système de demander le paiement ou l'autorisation immédiatement auprès de l'acquéreur (traitement en ligne), ou simplement de confirmer la réception de la transaction et de l'enregistrer pour que l'acquéreur puisse la saisir ultérieurement (traitement hors-ligne).

Le comportement de paiement est déterminé par des paramètres généraux que le marchand définit sous l'onglet « Paramètres de transaction globaux » sur la page d'information technique de son module d'administration : le code d'opération par défaut, la procédure de télécollecte par défaut (paiement) et le traitement pour les différentes transactions. Ces paramètres sont définis pour chaque compte ; ils s'appliquent par conséquent à l'ensemble des transactions effectuées sur le compte du marchand.

5.1 Code d'opération par défaut

IMPORTANT

La possibilité de travailler en deux étapes (autorisation + télécollecte) varie selon les moyens de paiement que vous souhaitez utiliser. (Voir l'aperçu en ligne Payment Methods Processing/Procedure)

Sur la base de ces deux étapes (« autorisation » et « télécollecte»), le marchand a le choix entre deux codes d'opération par défaut sous l'onglet « « Paramètres de transaction globaux », dans la rubrique Code d'opération par défaut » de la page d'information technique:

- Autorisation :

  Notre système effectue seulement une demande d'autorisation ; les deux étapes (autorisation et télécollecte (demande de paiement)) sont réalisées séparément à des moments différents (l'argent reste sur le compte du client jusqu'à ce qu'une télécollecte (demande de paiement) soit effectuée).

- Vente :

  Notre système demande automatiquement le paiement (transfert du montant) dès l'autorisation acceptée. Cette procédure est souvent utilisée pour les produits/services livrés en ligne.

5.2 Procédure de télécollecte (paiement) par défaut

IMPORTANT

La possibilité de travailler en deux étapes (autorisation + télécollecte) varie selon les moyens de paiement que vous souhaitez utiliser. (Voir l'aperçu en ligne Payment Methods Processing/Procedure)

Lorsque le marchand a opté pour le code d'opération par défaut « autorisation » pour son compte ou lorsqu'il a inclus le code d'opération « autorisation » dans les informations de transaction, une télécollecte doit être réalisée sur la transaction pour demander le paiement.

Il existe trois procédures de télécollecte (demande de paiement) possibles :

- télécollecte par le marchand (manuelle ou automatique) :

  Pour demander le transfert du montant réservé sur le compte bancaire du marchand, celui-ci

doit faire appel à son module d'administration et demander la télécollecte (paiement) pour la transaction concernée (veuillez vous reporter au Back Office User Guide).

Le marchand peut aussi automatiser le traitement de données en nous envoyant les télécollectespar batch ou par demande de serveur à serveur (veuillez vous reporter aux informations sur le Batch ou sur DirectLink).

La période de validité des autorisations varie selon le contrat conclu entre le marchand et son établissement acquéreur.

Cette procédure est souvent utilisée lorsque le marchand doit vérifier ses stocks avant d'expédier les produits commandés.

- télécollecte automatique par notre système en fin de journée :

  Notre système demande automatiquement le paiement (télécollecte) à partir de minuit, GMT+1.

- télécollecte automatique par notre système après x jours :

  Notre système demande automatiquement le paiement (télécollecte) après x jours (lorsque le marchand n'a pas annulé l'autorisation).

  Le nombre minimum de jours à définir est « 2 », puisque « 1 » reviendrait à demander automatiquement le paiement à partir de minuit.

  Cette procédure est souvent utilisée pour les produits/services livrés dans un délai déterminé (24 heures 48 heures, etc.).

5.3 Traitement pour les transactions individuelles

IMPORTANT

La possibilité de travailler en ligne ou hors-ligne varie selon les moyens de paiement que vous souhaitez utiliser. (Voir l'aperçu en ligne Payment Methods Processing/Procedure)

Il existe trois façons de traiter les transactions individuelles :

- Toujours en ligne (immédiat) :

  La demande de transaction est immédiatement envoyée à l'acquéreur alors que le client est connecté (convient pour les produits/services livrés en ligne).

  Lorsque le système de compensation en ligne de l'acquéreur est indisponible, toutes les transactions en ligne sont refusées.

- En ligne, mais passer à hors-ligne lorsque le système en ligne de l'acquéreur est indisponible :

  Lorsque le marchand souhaite opter pour un traitement en ligne mais ne veut pas risquer de passer à côté de transactions en cas d'indisponibilité temporaire du système de compensation en ligne de l'acquéreur, il peut autoriser un traitement hors-ligne dans ces circonstances bien précises.

  Dans ce cas, nous sauvegardons les transactions provenant du site Web du marchand pendant la période d'indisponibilité de son acquéreur pour les traiter hors-ligne dès que le système de compensation de l'acquéreur fonctionne à nouveau. (Ne convient pas pour les services qui sont livrés en ligne juste après la transaction !)

- Toujours hors-ligne (programmé) :

  Nous enregistrons la transaction et la traitons ultérieurement (4 heures plus tard max.). Cette méthode est un peu plus rapide pour le client puisque nous n'envoyons pas immédiatement la demande à l'acquéreur (peut être utilisée pour les produits/services qui ne doivent pas être livrés en ligne). Le client ne pourra cependant pas consulter immédiatement les résultats de la transaction/commande.

  Vous pouvez configurer une notification de changement de statut hors-ligne sous l'onglet « Retour d'information sur la transaction », dans la rubrique « Requête http pour les changements de statut » sur la page d'information technique de votre compte (pour les requêtes http) ou sous l'onglet « E-mails de transaction », dans la rubrique « E-pour le marchand » sur la page d'information technique (pour les e-mails). Cela vous permet d'être averti par e-mail et/ou demande http lorsque le statut d'une transaction est modifié et devient hors-ligne dans notre système.

6 Lien entre le site Web du marchand et notre page de paiement

6.1 Formulaire de commande

Le lien entre le site Web du marchand et notre page de paiement e-Commerce doit être établi sur la dernière page du panier d'achat sur le site du marchand, c'est-à-dire sur la dernière page de son site présentée au client.

Un formulaire contenant des champs html masqués contenant les informations sur la commande doit être intégré sur cette dernière page. L'URL d'action du formulaire est la page de traitement des paiements (de notre système e-Commerce).

6.1.1 Champs du formulaire

L'encadré ci-dessous contient le bloc de codage que le marchand doit copier sur la dernière page de son panier d'achat :

```
<form method="post" action="https://e-payment.postfinance.ch/ncol/test/orderstandard.asp" id=form1 name=form1>
<!—paramètres généraux : voir Parametres de paiement généraux -->
<input type="hidden" name="PSPID" value="">
<input type="hidden" name="ORDERID" value="">
<input type="hidden" name="AMOUNT" value="">
<input type="hidden" name="CURRENCY" value="">
<input type="hidden" name="LANGUAGE" value="">
<!—informations client facultatives, vivement recommandé à des fins de prévention de la fraude : voir Paramètres généraux et informations client facultatives -->
<input type="hidden" name="CN" value="">
<input type="hidden" name="EMAIL" value="">
<input type="hidden" name="OWNERZIP" value="">
<input type="hidden" name="OWNERADDRESS" value="">
<input type="hidden" name="OWNERCTY" value="">
<input type="hidden" name="OWNERTOWN" value="">
<input type="hidden" name="OWNERTELNO" value="">
<input type="hidden" name="COM" value="">
<!—vérification avant paiement : voir Signature SHA-IN -->
<input type="hidden" name="SHASIGN" value="">
<!—informations mise en page : voir Aspect de la page de paiement -->
<input type="hidden" name="TITLE" value="">
<input type="hidden" name="BGCOLOR" value="">
<input type="hidden" name="TXTCOLOR" value="">
<input type="hidden" name="TBLBGCOLOR" value="">
<input type="hidden" name="TBLTXTCOLOR" value="">
<input type="hidden" name="BUTTONBGCOLOR" value="">
<input type="hidden" name="BUTTONTXTCOLOR" value="">
<input type="hidden" name="LOGO" value="">
```

```
<input type="hidden" name="FONTTYPE" value="">
<!—modèle de page dynamique : voir Aspect de la page de paiement -->
<input type="hidden" name="TP" value="">
<!—moyens de paiement/caractéristiques page : voir Moyen de paiement et caractéristiques de la page de paiement -->
<input type="hidden" name="PM" value="">
<input type="hidden" name="BRAND" value="">
<input type="hidden" name="WIN3DS" value="">
<input type="hidden" name="PMLIST" value="">
<input type="hidden" name="PMListType" value="">
<!—lien vers votre site Web : voir Réaction par défaut -->
<input type="hidden" name="HOMEURL" value="">
<input type="hidden" name="CATALOGURL" value="">
<!—paramètres après paiement : voir Redirection en fonction du résultat du paiement -->
<input type="hidden" name="COMPLUS" value="">
<input type="hidden" name="PARAMPLUS" value="">
<!—paramètres après paiement : voir Requête de réponse directes (après paiement) -->
<input type="hidden" name="PARAMVAR" value="">
<!—redirection après paiement : voir Redirection en fonction du résultat du paiement -->
<input type="hidden" name="ACCEPTURL" value="">
<input type="hidden" name="DECLINEURL" value="">
<input type="hidden" name="EXCEPTIONURL" value="">
<input type="hidden" name="CANCELURL" value="">
<!—champ opération facultatif : voir Code Opération -->
<input type="hidden" name="OPERATION" value="">
<!-- champ facultatif informations complémentaires connexion : voir Champ Utilisateur -->
<input type="hidden" name="USERID" value="">
<!-- informations alias : voir document Alias Management -->
<input type="hidden" name="ALIAS" value="">
<input type="hidden" name="ALIASUSAGE" value="">
<input type="hidden" name="ALIASOPERATION" value="">
<input type="submit" value="" id=submit2 name=submit2>
</form>
```

Vous pouvez trouver un exemple (page test) représentant la dernière page du panier d'achat d'un marchand à l'adresse suivante : https://e-payment.postfinance.ch/ncol/test/teststd.asp.

Le marchand peut copier/coller le code html du formulaire situé en bas de sa page test sur la page de son panier d'achat. Les valeurs des champs doivent être remplacées par les valeurs du compte du marchand.

Certains champs (par ex., orderID et amount) doivent être attribués de manière dynamique.

6.1.2 Action du formulaire

<form method="post" action="https://e-payment.postfinance.ch/ncol/test/orderstandard.asp" id=form1 name=form1>

Dans l'environnement de Production, l'URL pour l'action sera https://e-payment.postfinance.ch/ncol/prod/orderstandard.asp.

IMPORTANT

Lorsque vous passez à votre compte de PRODUCTION, vous devez remplacer « test » par « prod » ; le formulaire d'action devient ainsi https://e-payment.postfinance.ch/ncol/prod/orderstandard.asp. Si vous oubliez de modifier l'action de votre formulaire, vos transactions seront envoyées à l'environnement test et non aux acquéreurs/banques lorsque vous commencerez à traiter de vraies commandes dans votre compte de production.

6.2 Paramètres généraux et informations client facultatives

Les paramètres généraux sont les paramètres qui doivent être envoyés avec chaque transaction pour nous permettre de les traiter.

Même si les paramètres obligatoires sont le PSPID, l'ID de la commande, le montant, la devise et la valeur langue, nous vous conseillons vivement de nous envoyer également certaines informations client facultatives, comme le nom du client, son adresse électronique, son adresse postale (ville, code postal, pays) et son numéro de téléphone – ces informations peuvent être utiles à des fins de lutte contre la fraude.

Ces informations client facultatives sont également enregistrées avec la transaction de notre côté et vous pourrez les analyser dans votre module d'administration en consultant les informations sur la transaction.

6.2.1 Champs masqués

Les champs masqués utilisés pour transmettre les paramètres généraux à notre système sont les suivants :

```
<input type="hidden" name="PSPID" value="">
<input type="hidden" name="ORDERID" value="">
<input type="hidden" name="AMOUNT" value="">
<input type="hidden" name="CURRENCY" value="">
<input type="hidden" name="LANGUAGE" value="">
<input type="hidden" name="CN" value="">
<input type="hidden" name="EMAIL" value="">
<input type="hidden" name="OWNERZIP" value="">
<input type="hidden" name="OWNERADDRESS" value="">
<input type="hidden" name="OWNERCTY" value="">
<input type="hidden" name="OWNERTOWN" value="">
<input type="hidden" name="OWNERTELNO" value="">
<input type="hidden" name="COM" value="">
```

Champ	Objet
PSPID	Votre nom d'affiliation dans notre système
ORDERID	Votre numéro de commande unique (référence marchand). Le système vérifie que les paiements ne sont pas demandés deux fois pour une même commande. Le champ orderID doit être attribué de

Champ	Objet
	manière dynamique.
AMOUNT	Montant à payer multiplié par 100 puisque le format du montant ne doit contenir aucune décimale ou autres séparateurs. Le montant doit être attribué de manière dynamique.
CURRENCY	Code ISO alpha de la devise de la commande, par exemple : EUR, USD, GBP, CHF, etc.
LANGUAGE	Langue du client, par exemple : en_US, nl_NL, fr_FR, etc.
CN	Nom du client. Pré-initialisé (mais néanmoins modifiable) dans le champ réservé au nom du titulaire de la carte dans les informations sur la carte de crédit.
EMAIL	Adresse électronique du client
OWNERADDRESS	Adresse postale (rue et n°) du client
OWNERZIP	Code postal du client
OWNERTOWN	Nom de la ville du client
OWNERCTY	Pays du client
OWNERTELNO	Numéro de téléphone du client
COM	Description de la commande

Pour des informations complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

7 Sécurité : vérification avant paiement

Meilleure pratique : Signature SHA-IN

7.1 Référant

Notre système vérifie l'origine de la demande de paiement, c.-à-d. l'URL d'où provient la commande. On appelle cet URL le « référant ».

7.1.1 Configuration

Le marchand indique le référant/l'URL de la page contenant le formulaire de commande avec les champs masqués dans le champ URL sous l'onglet « Contrôle de données et d'origine », dans la rubrique « Contrôles pour e-Commerce » de la page d'information technique de son compte.

Le/les URL(s) doi(ven)t toujours commencer par http:// ou https://. Vous pouvez saisir l'URL entier ou simplement le nom de domaine ; dans ce second cas, l'ensemble des sous-répertoires et des pages de ce domaine seront acceptés.

Le marchand peut saisir plusieurs URL s'il dispose de plusieurs domaines, par ex. « *http://www.mysite.com;http://www.mysite.net;http://www.secure.mysite.com* » Les URL doivent être séparés par un point-virgule (sans espaces avant ou après le point-virgule).

Lorsque vous effectuez une transaction test à partir de votre page test, veillez à saisir l'URL de notre site en guise de référant sans quoi un message d'erreur apparaîtra.

7.1.2 Erreurs possibles

Des erreurs liées au référant sont possibles, par ex., « *unknown order/1/r* » et « *unknown order/0/r* ». Veuillez vous reporter à l'Annexe: Dépannage pour de plus amples informations sur ces erreurs.

7.1.3 Contraintes

Le référant permet de vérifier l'origine d'une transaction, mais ne permet pas d'assurer l'intégrité des données. Pour cela, nous exigeons l'utilisation d'une signature SHA.

7.2 Signature SHA-IN

Cette technique se fonde sur le principe suivant : le serveur du marchand crée une chaîne de caractères unique, hachée par l'algorithme SHA, pour chaque commande. Le résultat de ce hachage nous est ensuite envoyé dans les champs masqués de la page de commande du marchand. Notre système reconstruit cette signature pour vérifier l'intégrité des informations de commande qui nous sont envoyées dans les champs masqués. Pour de plus amples informations sur la signature SHA, veuillez vous reporter à l'Annexe: SHA.

7.3 Vérification de l'adresse IP

Le champ consacré à l'adresse IP sous l'onglet « Contrôle de données et d'origine », dans la rubrique « Contrôles pour DirectLink et Batch (Automatique) » sur la page d'information technique, ne doit être rempli que s'il existe une connexion de serveur à serveur avec notre système à côté de la connexion e-Commerce (c.-à-d. demandes relatives à orderdirect.asp, maintenancedirect.asp, querydirect.asp, AFU_agree.asp).

Si cette option n'est pas utilisée, le champ peut rester vide. (Veuillez vous reporter à la documentation sur DirectLink / Batch Advanced).

8 Aspect de la page de paiement

Meilleure pratique : Présentation de la page de paiement (modèle statique)

Notre système e-Commerce demande au client de saisir les informations sur sa carte de paiement sur notre serveur sécurisé.

La page de traitement des paiements contient deux types d'informations : des informations statiques (le logo du marchand, par exemple) et les informations sur les données du paiement (référence de la commande, champs dans lesquels le client saisit les informations sur sa carte, etc ;).

Les informations statiques sont issues de la présentation classique dans notre système ou d'un modèle de page propre au marchand (comme expliqué plus loin). Notre système ajoute les données de paiement de façon dynamique pour chaque transaction. Le marchand peut néanmoins modifier l'aspect de ces données de paiement en utilisant des styles html.

Il existe deux façons de personnaliser le style de la page de traitement des paiements afin de préserver les caractéristiques visuelles du site du marchand durant le processus de paiement : en utilisant un modèle de page statique ou dynamique.

8.1 Présentation de la page de paiement (modèle statique)

Le modèle de page statique est un modèle commun que nous proposons, mais le marchand peut modifier l'aspect de certains éléments sur la page de paiement ou ajouter son logo ; il lui suffit pour cela d'ajouter quelques champs masqués dans le formulaire qu'il nous envoie (cf. chapitre 5) :

Les champs masqués utilisés pour transmettre les caractéristiques visuelles à notre système sont les suivants :

```
<input type="hidden" name="TITLE" value="">
<input type="hidden" name="BGCOLOR" value="">
<input type="hidden" name="TXTCOLOR" value="">
<input type="hidden" name="TBLBGCOLOR" value="">
<input type="hidden" name="TBLTXTCOLOR" value="">
<input type="hidden" name="BUTTONBGCOLOR" value="">
<input type="hidden" name="BUTTONTXTCOLOR" value="">
<input type="hidden" name="LOGO" value="">
<input type="hidden" name="FONTTYPE" value="">
```

Champ	Objet	Valeur par défaut
TITLE	Titre et en-tête de la page	_
BGCOLOR	Couleur de fond	blanc
TXTCOLOR	Couleur du texte	noir
TBLBGCOLOR	Couleur de fond du tableau	blanc
TBLTXTCOLOR	Couleur du texte du tableau	noir
BUTTONBGCOLOR	Couleur de fond du bouton	_
BUTTONTXTCOLOR	Couleur du texte du bouton	noir
FONTTYPE	Famille de police	Verdana

Champ	Objet	Valeur par défaut
LOGO	URL/Nom de fichier du logo que vous voulez afficher en haut de la page de paiement à côté du titre. L'URL doit être absolu (contient le chemin complet), il ne peut pas être relatif. Si vous ne possédez pas un environnement sécurisé pour enregistrer votre image, vous pouvez envoyer un fichier JPG, PNG ou GIF (et votre PSPID) à merchanthelp@postfinance.ch. Veuillez prendre contact avec notre service à la clientèle Merchanthelp, en composant le +41 (0)848 38 24 23, ou par E-mail : merchanthelp@postfinance.ch pour activer l'option "Logo Hosting" dans votre Compte. Si le logo est enregistré sur nos serveurs, l'URL sera https://e-payment.postfinance.ch/images/merchant/*[PSPID]*/*[image]*	_

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

Vous pouvez définir les couleurs par leur code hexadécimal (#FFFFFF) ou par leur nom (« white »). Vérifiez d'abord l'apparence des couleurs que vous souhaitez utiliser dans différents navigateurs.

8.1.1 Modèle statique pour iPhone

Nous avons développé un modèle particulier pour les iPhones sur notre plateforme. Pour utiliser notre modèle statique pour iPhone, il vous suffit de nous transmettre l'URL du modèle de page pour iPhone au moyen du champ masqué et de la valeur suivants :

```
<input type="hidden" name="TP" value="template_STD_postfinance_1_mobile.htm">
```

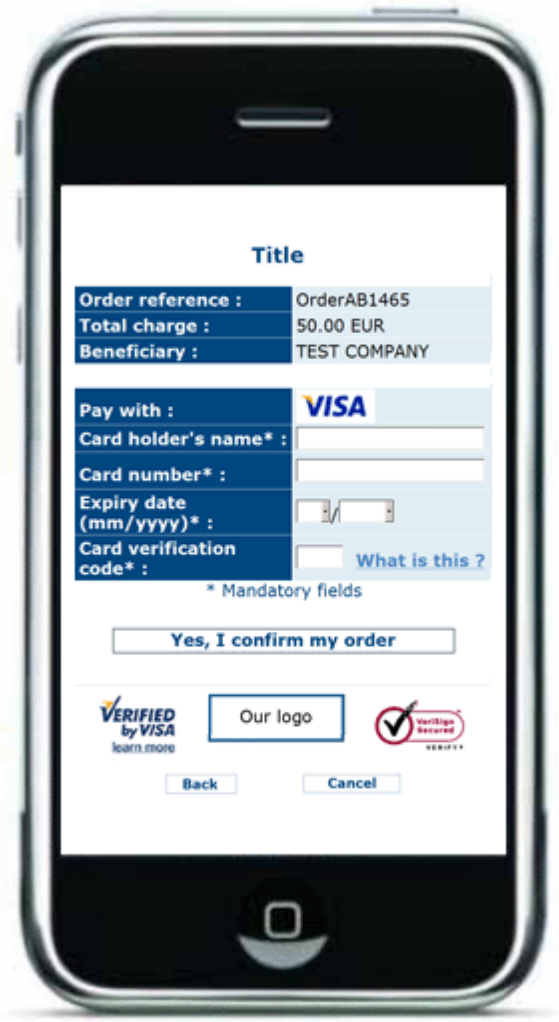
IMPORTANT

Nous nous engageons sur la compatibilité de nos pages de paiement sécurisé avec l'iPhone. Nous ne pouvons garantir que toutes les pages externes accessibles via nos pages de paiement (par ex., les sites tiers ou les sites de banques) le soient.

L'interface de saisie de données est adaptée à la taille de l'écran de l'iPhone. Le marchand peut personnaliser les caractéristiques visuelles selon ses besoins ; il lui suffit pour cela d'ajouter quelques champs masqués dans le formulaire qu'il nous envoie. Les champs masqués utilisés pour transmettre les caractéristiques visuelles du modèle pour iPhone à notre système sont les suivants :

```
<input type="hidden" name="TITLE" value="">
<input type="hidden" name="BGCOLOR" value="">
<input type="hidden" name="TXTCOLOR" value="">
<input type="hidden" name="TBLBGCOLOR" value="">
<input type="hidden" name="TBLTXTCOLOR" value="">
<input type=”hidden” name=”HDTBLBGCOLOR” value=””>
<input type=”hidden” name=”HDTBLTXTCOLOR” value=””>
<input type=”hidden” name=”HDFONTTYPE” value=””>
<input type="hidden" name="BUTTONBGCOLOR" value="">
<input type="hidden" name="BUTTONTXTCOLOR" value="">
<input type="hidden" name="FONTTYPE" value="">
```

Champ	Objet	Valeur par défaut
TITLE	Titre de la page	_
BGCOLOR	Couleur de fond	#FFFFFF
TXTCOLOR	Couleur du texte	#00467F
TBLBGCOLOR	Couleur de fond pour les colonnes de droite	#E1EDF4
TBLTXTCOLOR	Couleur du texte pour les colonnes de droite	#000000
HDTBLBGCOLOR	Couleur de fond pour les colonnes de gauche	#00467F
HDTBLTXTCOLOR	Couleur du texte pour les colonnes de gauche	#FFFFFF
HDFONTTYPE	Famille de police pour les colonnes de gauche	Verdana
BUTTONBGCOLOR	Couleur de fond du bouton	#FFFFFF
BUTTONTXTCOLOR	Couleur du texte du bouton	#00467F
FONTTYPE	Famille de police	Verdana



8.2 Mise en page basée sur le modèle (modèle dynamique)

Le modèle de page dynamique est une technique avancée permettant de personnaliser l'apparence des pages de paiement. L'utilisation du modèle dynamique est limitée à certains abonnements. Si cette option vous intéresse et qu'elle n'apparaît pas dans la liste d'options de votre page d'abonnement dans votre compte, contactez notre service clientèle Merchanthelp, Tel. +41 (0)848 38 24 23, E-Mail: merchanthelp@postfinance.ch.

Lorsque le marchand utilise un modèle de page dynamique, c'est lui qui définit entièrement l'apparence de son modèle de page ; seule une zone sur cette page est complétée par notre système. L'URL du modèle de page du marchand doit nous être envoyé dans les champs masqués pour chaque transaction. Rappelez-vous que si vous utilisez un modèle de page dynamique, notre système devra envoyer une demande supplémentaire afin de consulter votre modèle de page, ce qui allonge le processus de paiement.

8.2.1 Champs masqués

Le champ masqué utilisé pour transmettre l'URL de votre modèle de page est le suivant :

```
<input type="hidden" name="TP" value="">
```

Champ	Objet
TP	URL du modèle de page dynamique du marchand (la page doit être hébergée du

Champ	Objet
	côté du marchand). L'URL doit être absolu (il doit contenir le chemin complet), et non relatif. Ne précisez aucun port dans votre URL : nous n'acceptons que les ports 443 et 80. Toute composante incluse dans le modèle de page tout aussi avoir un URL absolu.

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au Parameter Cookbook en ligne.

8.2.2 Zone de paiement

Vous pouvez concevoir l'ensemble du modèle de page dynamique selon vos préférences. La seule condition à observer est qu'il doit contenir la chaîne « $$$PAYMENT ZONE$$$ », qui indique l'endroit où notre module e-Commerce peut ajouter ses champs de manière dynamique. Il doit par conséquent contenir au moins les champs suivants :

```
<html>
$$$PAYMENT ZONE$$$
</html>
```

IMPORTANT

N'utilisez pas de balises BASE, de cadres ou de balises FORM pour encapsuler la chaîne $$$PAYMENT ZONE$$$.

Exemple

Vous trouverez un exemple de modèle de page dynamique à l'adresse suivante :

https://e-payment.postfinance.ch/ncol/template_standard.htm

8.2.3 Comportement dynamique

Le marchand peut opter pour un même modèle de page pour toutes les commandes ou pour un modèle produit de manière dynamique par son application en fonction des paramètres de la commande.

Pour produire le modèle de page de façon dynamique, le marchand a deux possibilités : créer une page propre à la commande, dont l'URL est transmis dans les champs masqués, ou utiliser un URL fixe mais produisant un résultat découlant du numéro de commande. Pour cela, notre système ajoute les principales données de paiement (y compris le numéro de référence de la commande du marchand) (cf. Traitement après paiement) lorsqu'il récupère le modèle de page :

HTTP request = url_page_template ?orderID=...&amount=...&currency=…

8.2.4 Feuille de style

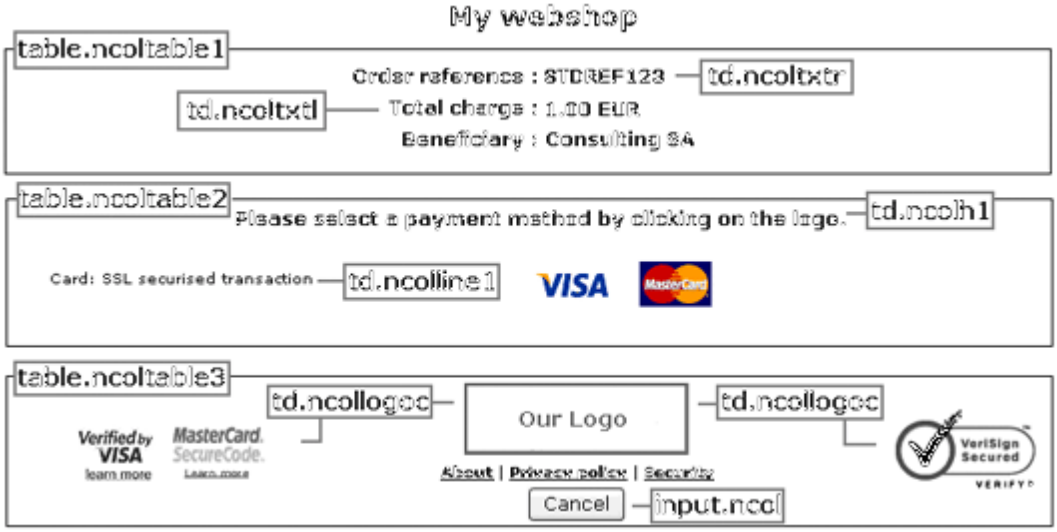
Vous pouvez personnaliser l'aspect de vos pages de paiement en ajoutant des feuilles de style à votre modèle de page.

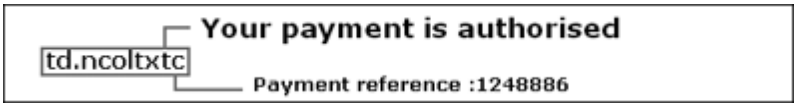
Nous avons défini une catégorie pour les différents types de tableaux et de cellules contenues dans nos tableaux, ainsi qu'une catégorie pour les boutons d'envoi. Ajoutez les blocs de codage suivants entre les balises <head></head> et modifiez les propriétés de ces catégories pour les adapter à l'aspect de votre site (voir l'exemple du modèle de page mentionné plus haut) :

```
<style type="text/css">
<!--
td.ncolh1 {background-color : #006600; color : yellow; font-family : verdana}
td.ncoltxtl {background-color : #ffffcc; color : black; text-align : right; font-weight : bold}
```

```
td.ncoltxtl2 {background-color : #ffffcc; color : black; text-align : right; font-weight : bold}
td.ncoltxtr {background-color : #ffffcc; color : black; text-align : left; font-weight : bold}
td.ncoltxtc {background-color : #ffffcc; color : black; text-align : center; font-weight : bold}
td.ncolinput {background-color : #ffffcc; color : black}
td.ncolline1 {background-color : #ffffff; color : black}
td.ncolline2 {background-color : #ffffcc; color : black}
input.ncol {background-color : #006600; color : white}
td.ncollogoc {background-color : #ffffcc; color : black; text-align : center; font-weight : bold}
table.ncoltable1 { background-color: #ffffcc;   }
table.ncoltable2 { background-color: #ffffcc;  border-width : medium; border-color : green; }
table.ncoltable3 { background-color: #ffffcc; }
-->
</style>
```

Lors de la saisie de vos instructions de mise en page, vous devez respecter la syntaxe de la feuille de style en cascade. Nous vous conseillons vivement de tester votre présentation dans différents navigateurs. La façon dont ils traitent les styles peut en effet énormément varier.





8.2.5 Performance

La configuration de notre système prévoit un délai de 5 secondes pour la demande de récupération de la page correspondant au modèle dynamique du marchand.

Veuillez contacter notre notre service clientèle Merchanthelp, Tel. +41 (0)848 38 24 23, E-Mail: merchanthelp@postfinance.ch, pour changer cette valeur (HTTPTimeOut).

Si ce délai est dépassé, notre système utilise le modèle statique du marchand.

Si aucun modèle statique n'est configuré, notre système utilise en dernier ressort le modèle statique de PostFinance.

IMPORTANT

Ce champ HTTPTimeOut a une incidence non seulement sur les demandes de modèle dynamique, mais aussi sur les demandes d'informations après paiement (voir Requête de réponse directes (après paiement)). En conséquence, si le marchand décide de le modifier pour le faire passer à 15 secondes, par exemple, la temporisation pour la demande d'informations passera elle aussi à 15 secondes.

Pour chaque commande, notre système effectue une demande de récupération de votre modèle de page dynamique. Si vos volumes de transaction sont importants ou si votre modèle de page est lourd (par ex., s'il contient un grand nombre d'images), ces demandes http peuvent être longues. Contactez notre service clientèle Merchanthelp pour trouver une solution si vos volumes de transaction sont importants.

8.3 Contrôle de la sécurité des modèles

Pour protéger les clients du commerçant des activités frauduleuses telles que la manipulation des données sensibles de la carte (numéro de carte, code de vérification CVC), différents contrôles de sécurité ont été mis à disposition pour le modèle du commerçant.

Sur la page Information technique du commerçant, onglet "Paramètres globaux de sécurité", section "Modéle", vous pouvez configurer les paramètres suivants :

- Contrôle JavaScript sur le modèle
  Le commerçant peut activer cette fonction pour détecter l'utilisation de Javascript sur la page du modèle.Si Javascript est détecté, le modèle est bloqué et c'est le modèle par défaut qui est utilisé.
- l'Utilisation d'un modèle statique
  Le commerçant peut sélectionner quels types de modèles sont autorisés pour lancer une transaction sur notre plate-forme :les types statique et dynamique peuvent tous deux être configurés.

- Si le commerçant a activé l'option *Autoriser l'utilisation d'un modèle statique*, il est obligatoire de définir le nom du modèle statique de confiance. Cette liste sera utilisée comme entrée lors d'un contrôle qui consistera à la comparer aux informations reçues par PostFinance au cours du processus de paiement. Vous pouvez entrer ici une ou plusieurs valeurs, séparées par un point-virgule.
- Si le commerçant a activé l'option *Autoriser l'utilisation d'un modèle dynamique*, il est obligatoire de définir le nom d'hôte du site web de confiance qui héberge ce modèle dynamique. Ce champ peut contenir plusieurs noms d'hôte, séparés par un point-virgule, mais ils doivent tous contenir l'adresse URL complète, p. ex. http://www.website.com/. Les sous-répertoires peuvent être omis, de telle sorte que si le modèle dynamique est http://www.website.com/templates/nl/template1.htm, il suffit de définir http://www.website.com comme nom d'hôte du site web de confiance.

  En outre, le commerçant peut également définir, s'il le souhaite, une ou plusieurs adresses URL de modèle dynamique totalement fiables, séparées par un point-virgule.

Si un modèle dynamique est soumis lors d'une transaction, mais que les modèles dynamiques ne sont pas autorisés, le modèle sera bloqué et notre système utilisera à sa place le modèle statique.

Si aucun modèle statique n'a été défini ou si le modèle statique est également interdit d'utilisation, c'est le modèle PostFinance par défaut qui sera utilisé.

IMPORTANT

Si un modèle statique ou dynamique par défaut est configuré dans le compte du commerçant (cela ayant fait l'objet d'une demande préalable à our customer care Merchanthelp), il convient d'activer une des 2 options (*Autoriser l'utilisation d'un modèle statique* / *Autoriser l'utilisation d'un modèle dynamique)*. L'URL du modèle doit également être définie comme *modèle de confiance*. Si le champ d'entrée *URL du modèle statique/dynamique de confiance* reste vide, tous les modèles sont considérés comme fiables par défaut.

Par défaut, les options C*ontrôle JavaScript sur le modèle* et *l'Utilisation d'un modèle statique* sont activées pour les commerçants. Le champ *Nom du modèle statique de confiance* est prédéfini selon le nom d'hôte du site web du commerçant.

8.4 Cadenas de l'environnement sécurisé

L'URL utilisé pour connecter le client à notre plateforme utilise un protocole sécurisé (https). L'ensemble des communications entre notre plateforme e-Commerce et le client sont chiffrées de façon sécurisée.

Il arrive cependant que le cadenas du navigateur (qui signale au client que le site est sécurisé) n'apparaisse pas lorsque certains éléments (comme des images) contenus sur le modèle de page ne sont pas hébergés sur un serveur sécurisé ou lorsque certains frame sur l'écran présentent des pages qui ne proviennent pas de sites sécurisés.

Même si la communication liée au traitement des paiements est chiffrée, la plupart des navigateurs ne reconnaissent les connexions sécurisées que si tous les éléments apparaissant à l'écran (images, sons, etc.) proviennent de sites sécurisés.

Pour les marchands qui ne disposent pas d'un site sécurisé, souvenez-vous des règles suivantes :

1. N'utilisez pas de *frames* pour les pages de paiement : vous pouvez actualiser l'ensemble de l'écran avec un modèle de page qui donne l'impression que vous utilisez des cadres ou faire en sorte que le paiement puisse être traité dans une nouvelle fenêtre.
2. Ne liez pas de fichiers au modèle de page (balise <link>) que vous utilisez pour la page de paiement. Utilisez plutôt les balises <style> et <script> pour intégrer des styles et des scripts sur le modèle de page.
3. Assurez-vous que les images de votre modèle sont hébergées sur un serveur sécurisé (le modèle de page peut être hébergé sur un serveur non sécurisé, mais pas les images). Nous pouvons nous héberger ces éléments (consultez les options d'hébergement des images dans votre compte).

8.5 Bouton "Annuler"

Un bouton « Annuler » est présent par défaut sur nos pages de paiement sécurisé afin de permettre au client d'annuler/interrompre sa transaction. Si vous souhaitez masquer ce bouton, vous pouvez cocher la case correspondante sous l'onglet « Affichage de la page de paiement » sur la page d'information technique de votre compte.

8.6 Page de paiement dans un iFrame

l'utilisation d'iframes devient de plus en plus populaire. ils permettent aux marchands d'intégrer une page externe (tel que la page de paiement) dans leur interface, tout en maintenant leur propre URL dans la barre d'adresse du navigateur.

Cependant, dans le contexte actuel, les iframes ont plusieurs désavanatages non-négligeables:

- Comme l'URL est celle du marchand, elle peut être http (au lieu d'https) sans afficher l'icône du cadenas dans la navigateur. Cela peut provoquer un sentiment de doute chez le porteur de carte quand à la sécurité de sa transaction;
- Certaines méthodes de paiement (comme Giropay, Sofortüberweisung, Bancontact/Mister Cash, PayPal...) utilisent des redirections vers des sistes externes, ce qui peut provoquer des gros soucis de mise en page et de navigation

Pour ces raisons, PostFinance déconseille formellement l'utilisation des iframes, et leur utilisation est

aux risques et périls du marchand. Nous conseillons l'utilisation de Modèles Dynamiques comme alternative.

Si vous souhaitez rtout de même utiliser un iframe, veuillez noter les recommendations suivantes

- Utilisez des iframes uniquement pour la page de paiement et au-dela
- Quand vous en avez la possibilité, utilisez des pop-ups dès que possible, afin d'assurer la visibilité des applications de tierces parties.

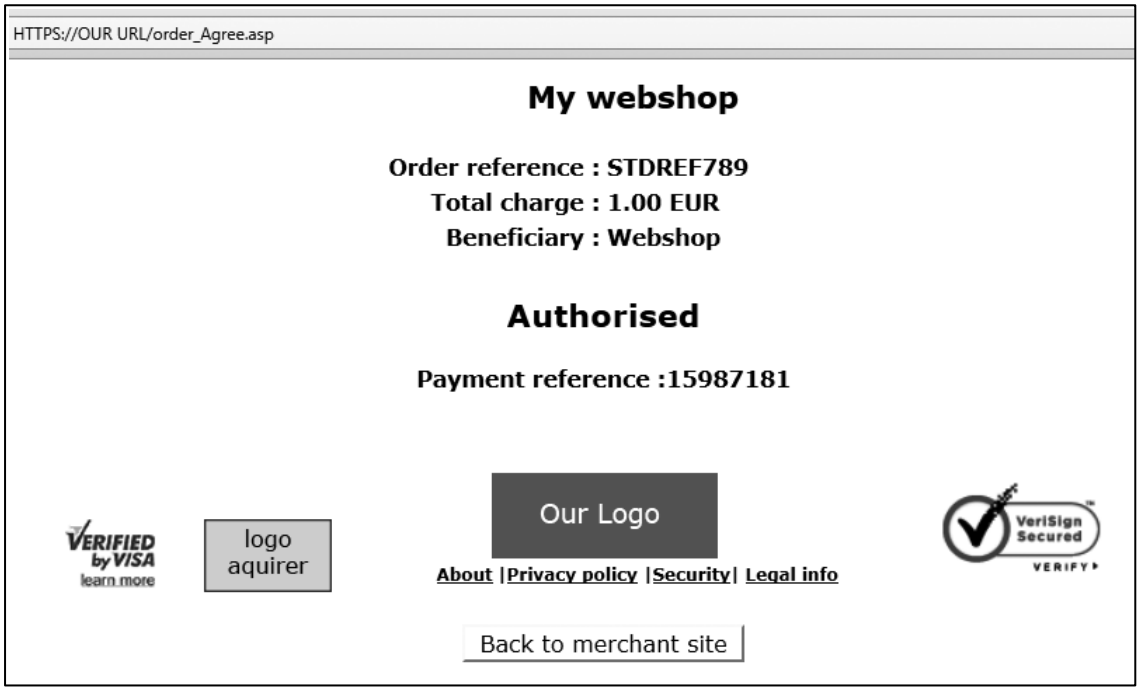
9 Informations sur la transaction transmises au client et au marchand

Meilleure pratique : Redirection avec paramètres sur accept-/exception-/cancel-/ declineurl (voir Option mise à jour de la base de données) avec une demande d'informations après-paiement différée pour plus de sécurité (voir Association avec une requête de réponse) et une vérification SHA-OUT par le marchand (voir Signature SHA-OUT (pour les demandes d'information et les redirections)).

Les informations transmises au marchand et à son client (lorsque le paiement est accepté, que le client a annulé le paiement ou que l'acquéreur a refusé le paiement plus que le nombre de fois autorisé) varient selon les paramètres définis par le marchand.

9.1 Réaction par défaut

Lorsque le marchand n'a défini aucune réaction particulière, notre système affiche le message standard pour le client : « Your payment is authorized » (votre paiement est autorisé) ou « The transaction has been denied » (la transaction a été refusée). Ce message est intégré dans le modèle de page.



Sur cette page, nous ajoutons également un lien vers le site du marchand et/ou le catalogue du marchand grâce aux URL (homeurl et catalogurl) envoyés dans les champs masqués du formulaire de commande. Lorsque ces URL ne sont pas précisés dans les champs masqués, notre système utilise l'URL indiqué dans le module de gestion de votre compte (compte > étape 1).

9.1.1 Champs masqués

Les champs masqués utilisés pour transmettre les URL sont les suivants :

```
<input type="hidden" name="CATALOGURL" value="">
<input type="hidden" name="HOMEURL" value="">
```

Champ	Objet
CATALOGURL	URL (absolu) de votre catalogue. Une fois la transaction traitée, votre

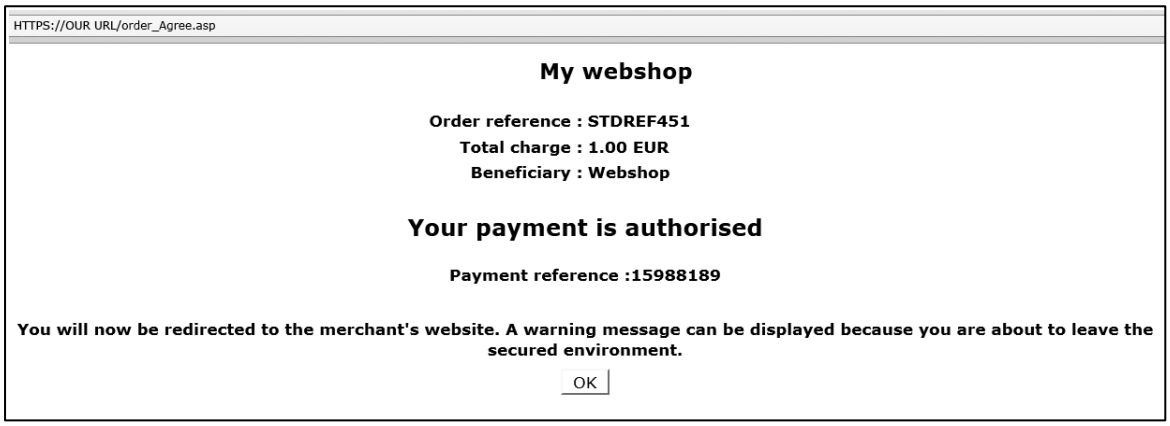
Champ	Objet
	client est invité à revenir à cet URL en cliquant sur un bouton.
HOMEURL	URL (absolu) de votre page d'accueil. Une fois la transaction traitée, votre client est invité à revenir à cet URL en cliquant sur un bouton. Lorsque vous envoyez la valeur « NONE» (néant), le bouton ramenant le client au site du marchand est masqué.

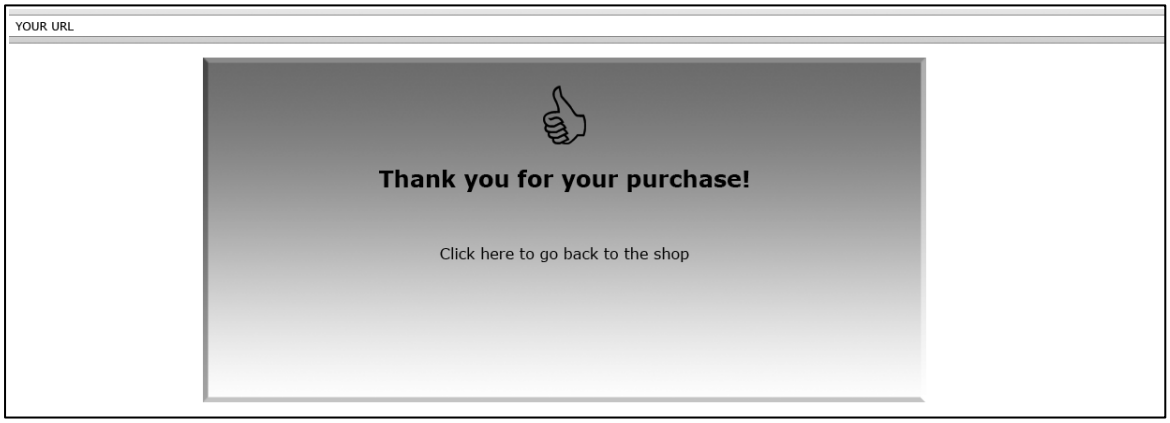
Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

9.2 Redirection en fonction du résultat du paiement

Dans les champs masqués de son formulaire de commande, le marchand peut envoyer 4 URL (accepturl, exceptionurl, cancelurl et declineurl) vers lesquels notre système redirige le client au terme du processus de paiement. Le marchand peut aussi configurer ces URL sous l'onglet « Retour d'information sur la transaction », dans la rubrique « redirection HTTP dans le navigateur » de la page d'information technique.

Exemple d'utilisation d'un « accepturl » pour personnaliser la réponse transmise au client :





9.2.1 Champs masqués

Les champs masqués utilisés pour transmettre les URL sont les suivants :

<input type="hidden" name="ACCEPTURL" value="">

<input type="hidden" name="DECLINEURL" value="">

<input type="hidden" name="EXCEPTIONURL" value="">

<input type="hidden" name="CANCELURL" value="">

Champ	Objet
ACCEPTURL	URL de la page Web à présenter au client une fois le paiement autorisé (statut 5), enregistré (statut 4), accepté (statut 9) ou en attente d'une acceptation (en attente, statut 41, 51 ou 91).
DECLINEURL	URL de la page Web à présenter au client lorsque l'acquéreur refuse l'autorisation (statut 2 ou 93) plus que le nombre de fois maximum autorisé.
EXCEPTIONURL	URL de la page Web à présenter au client lorsque le résultat du paiement est incertain (statut 52 ou 92). Si ce champ est vide, l'accepturl sera présenté au client en lieu et place.
CANCELURL	URL de la page Web à présenter au client lorsqu'il annule le paiement (statut 1). Si ce champ est vide, le declineurl sera présenté au client en lieu et place.

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

9.2.2 Alerte navigateur

Lorsqu'un client quitte nos pages de paiement sécurisé pour revenir sur le site du marchand, il est possible que son navigateur l'avertisse qu'il va pénétrer dans un environnement non sécurisé (étant donné qu'il passé d'un environnement https:// à un environnement http://). Lorsque nous détectons une redirection vers le site du marchand, nous pouvons afficher un message pour signaler au client qu'il est possible qu'un avertissement apparaisse (voir la première capture d'écran au chapitre Redirection en fonction du résultat du paiement), afin de lui éviter de s'inquiéter inutilement lorsque l'alerte apparaîtra dans son navigateur. Le marchand peut activer cette option sous l'onglet « Retour d'information sur la transaction », dans la rubrique « Redirection HTTP dans le navigateur » de la page d'information technique (*« Je veux que PostFinance affiche, sur la page de paiement, un message court à l'attention du client lorsqu'une redirection vers votre site est détectée juste après le processus de paiement.»*)

9.2.3 Option mise à jour de la base de données

Le marchand peut utiliser cette redirection sur accept-/exception-/cancel-/declineurl pour déclencher des tâches administratives automatiques, comme des mises à jours de bases de données. Lorsqu'un paiement est exécuté, nous pouvons envoyer les paramètres de la transaction sur les accept-, exception-, cancel- or declineurl du marchand.

Le marchand peut activer cette option sous l'onglet « Retour d'information sur la transaction », dans la rubrique « Redirection HTTP dans le navigateur » sur la Page d'information technique (*« Je veux recevoir les paramètres de transaction en retour dans les URL lors de la redirection.»*)

Notez que nous activons toujours la requête serveur-serveur (voir chapitre Informations sur la transaction transmises au client et au marchand) pour éviter les incohérences entre le paiement et la commande dues à une manipulation du client (ex: le client ferme son navigateur avant d'avoir reçu confirmation de l'autorisation)

9.2.3.1 Paramètres du retour d'information

Lorsqu'un paiement est exécuté, nous pouvons envoyer la liste de paramètres suivants sur les accept-, exception-, cancel- or declineurl du marchand.

Paramètre	Valeur
orderID	Votre référence de commande

Paramètre	Valeur
amount	Montant de la commande (pas multiplié par 100)
currency	Devise de la commande
PM	Moyen de paiement
ACCEPTANCE	Code d'acceptation produit par l'acquéreur
STATUS	Statut de la transaction (voir Annexe: Bref aperçu des statuts)
CARDNO	Numéro masqué de la carte
PAYID	Référence du paiement dans notre système
NCERROR	Code d'erreur
BRAND	Marque de la carte (notre système se base pour cela sur le numéro de carte)
ED	Date d'expiration
TRXDATE	Date de la transaction
CN	Nom du titulaire de la carte/client
SHASIGN	Signature SHA calculée par notre système (si configuré sur SHA-1-OUT)

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

La liste des paramètres des informations peut être plus longue pour les marchands qui ont activé certaines options dans leurs comptes, comme le module de détection de fraude. Veuillez vous reporter à la documentation sur l'option concernée pour de plus amples informations sur les autres paramètres des informations liés à l'option.

Exemple

https://www.yourwebsite.com/acceptpage.asp?orderID=ref12345&currency=EUR&amount=25&PM=CreditCard&ACCEPTANCE=test123&STATUS=5&CARDNO=XXXXXXXXXXXX1111&PAYID=1136745&NCERROR=0&BRAND=VISA&ED=0514&TRXDATE=12/25/08&CN=John Doe

Le marchand peut nous envoyer deux paramètres supplémentaires dans les champs masqués du formulaire de commande afin de les récupérer en tant que paramètres des informations au terme du paiement. Les champs masqués suivants sont proposés :

<input type="hidden" name="COMPLUS" value="">

<input type="hidden" name="PARAMPLUS" value="">

Champ	Objet
COMPLUS	Champ servant à soumettre une valeur que vous aimeriez récupérer dans la demande d'informations.
PARAMPLUS	Champ servant à soumettre certains paramètres et leurs valeurs que vous aimeriez récupérer dans la demande d'informations. Le champ paramplus n'est pas inclus dans les paramètres des informations proprement dits ; les paramètres/valeurs que vous soumettez dans ce champ seront

Champ	Objet
	en revanche analysés et les paramètres ainsi obtenus, ajoutés à la demande http.

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

Exemple

Les champs masqués supplémentaires envoyés par le marchand sont les suivants :

<input type="hidden" name="complus" value="123456789123456789123456789">

<input type="hidden" name="paramplus" value="SessionID=126548354&ShopperID=73541312">

Entraîne une redirection avec paramètres des informations :

https://www.yourwebsite.com/acceptpage.asp?[...*paramètres standard*...]

&COMPLUS=123456789123456789123456789&SessionID=126548354&ShopperID=73541312

9.2.3.2 Mesures de sécurité

Le processus de redirection est visible car il passe par le navigateur du client. Le marchand doit par conséquent utiliser une signature SHA (voir Annexe: SHA) pour vérifier le contenu de la demande et empêcher les clients de toucher aux données dans le champ URL, ce qui pourrait entraîner des mises à jour de bases de données frauduleuses. Si le marchand ne configure pas de signature SHA-OUT, nous n'enverrons aucun paramètre sur son accept-, exception-, cancel- or declineurl.

9.2.3.3 Association avec une requête de réponse

Le marchand est obligé d'utiliser - en plus des paramètres de retour vers les accept-/exception-/cancel-/declineurl - une requête différée comme garde-fou en cas d'échec de la redirection (voir Requête de réponse directes (après paiement)).

En cas d'interruption de la communication avec le client, par exemple lorsque le client ferme la fenêtre de son navigateur avant d'atteindre les accept-, exception-, cancel- ou declineurl, le marchand ne reçoit pas la redirection sur les accept-, exception-, cancel- ou declineurl. Cependant, si le marchand saisit un URL d'après-paiement sous l'onglet « Retour d'information sur la transaction » dans la rubrique « Requête directe http serveur-à-serveur » (champs URL) sur la page d'information technique et règle la planification de la demande sur « Toujours offline (hors ligne, différé) », il reçoit une réponse différée peu de temps après la transaction.

Pour que cela fonctionne, la page d'après-paiement du marchand doit pouvoir accepter les demandes pour les commandes qui ont déjà été traitées. Le marchand reçoit dans tous les cas cette demande d'informations différée, même en cas d'échec de la redirection sur les accept-, exception-, cancel- ou declineurl. Cette seconde demande peut être ignorée lorsque le statut de la commande a déjà été mis à jour dans la base de données du marchand à la suite de la redirection sur les accept-, exception-, cancel- or declineurl.

9.3 Requête de réponse directes (après paiement)

Après le paiement, notre système peut envoyer une demande http à un URL défini par le marchand et transmettre les données de transaction.

Ce processus permet au marchand de mettre à jour sa base de données en y intégrant le statut de la commande, etc. et de déclencher un processus de « fin de commande » (si cela n'a pas encore été fait après une redirection). C'est aussi une autre façon de générer une réponse personnelle pour le client en cas de besoins particuliers (si cela n'a pas encore été fait par le biais d'une redirection).

9.3.1 URL et paramètres d'après-paiement

9.3.1.1 URL d'après-paiement

Si vous souhaitez automatiser vos tâches administratives, vous pouvez définir les URL de deux pages exécutables sur votre site sous l'onglet « Retour d'information sur la transaction », dans la rubrique « Requête directe http serveur-à-serveur » (champs URL) de la page d'information technique. Vous pouvez par exemple indiquer l'URL sur lequel vous recevez les paramètres dans une demande lorsque le statut du paiement est accepté, en attente ou incertain. L'autre URL sera par exemple celui sur lequel vous souhaitez recevoir les paramètres dans une demande lorsque la transaction a été annulée par le client ou refusée trop de fois par l'acquéreur (c.-à-d. plus que le nombre de tentatives de paiement autorisé, tel que défini sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Tentatives de paiement multiples » de la page d'information technique). Ces deux URL peuvent être différents, mais ils peuvent aussi être identiques. Vous pouvez aussi saisir un URL pour le premier cas et aucun pour le second. N'indiquez aucun port dans votre URL ; nous n'acceptons que les ports 443 et 80.

Si vous souhaitez aussi recevoir une demande http différée en cas de changement de statut d'une transaction, vous pouvez indiquer un URL supplémentaire dans le champ sous l'onglet « Retour d'information sur la transaction », dans la rubrique « requête http les pour changements de statut » de la page d'information technique (et sélectionner une planification pour la demande). Ce processus est similaire aux URL d'après-paiement, à la différence qu'il convient pour les processus d'arrière-plan éventuels. Vous pouvez utiliser le même URL ici que celui défini dans la rubrique « Requête directe HTTP serveur-à-serveur », mais rappelez-vous qu'il est vain de l'utiliser pour générer une réponse personnelle pour le client dans ce cas (arrière-plan).

9.3.1.2 URL d'après-paiement variables

Si vous avez configuré une page d'après-paiement sur la page d'information technique de votre compte, mais que vous disposez de plusieurs boutiques qui sont chacune connectée à un répertoire déterminé pour recevoir les informations d'après-paiement, vous pouvez rendre une partie de votre URL d'après-paiement variable.

Cette partie variable peut aussi servir, par exemple, à « adapter » la demande d'informations pour inclure des informations sur la session, en les faisant passer comme une partie de l'URL plutôt que comme un paramètre supplémentaire. C'est le cas pour les plateformes Intershop ou les systèmes Servlets.

Le champ masqué à utiliser est le suivant :

<input type="hidden" name="PARAMVAR" value="">

Champ	Objet
PARAMVAR	La partie variable à intégrer dans les URL utilisés pour les demandes d'informations

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au Parameter Cookbook en ligne.

Exemple

URL d'après paiement sur la page d'information technique du marchand :

https://www.yourwebsite.com/<PARAMVAR>/yourpage.asp

Le champ masqué supplémentaire envoyé par le marchand est le suivant :

<input type="hidden" name="PARAMVAR" value="shop1">

Ce qui donne l'URL d'après paiement suivant pour la transaction :

https://www.yourwebsite.com/shop1/yourpage.asp

9.3.1.3 Paramètres des informations

Notre demande http envoyée vers votre URL d'après paiement contiendra les mêmes paramètres d'informations que ceux décrits au chapitre Paramètres du retour d'information.

9.3.2 Plannification de la requête d'informations

Sous l'onglet « Retour d'information sur la transaction », dans la rubrique « Requête directe HTTP serveur-à-serveur » de la page d'information technique de votre compte, vous pouvez définir le moment où la requête contenant les informations doit être envoyée :

- Aucune :

  Le marchand ne peut choisir cette option car il est obligé de recevoir les requêtes serveur-serveur (voir Informations sur la transaction transmises au client et au marchand).

- Toujours différée (pas immédiatement après le paiement) :

  La requête contenant les informations est envoyée peu de temps après la fin du processus de paiement. Elle est alors une tâche de fond et ne peut pas servir à envoyer des informations personnalisées au client sur le site du marchand.

  Lorsque le marchand n'utilise pas sa page d'après-paiement pour définir une réponse personnalisée à envoyer à son client, il peut recevoir la requête contenant les informations en arrière plan et de façon différée.

- Toujours en ligne (immédiatement après le paiement pour pouvoir personnaliser la réponse affichée pour le client) :

  La requête contenant les informations est envoyée « en ligne » entre le moment où notre système reçoit la réponse de l'acquéreur et le moment où il informe le client du résultat du paiement.

  Dans ce cas, le processus de paiement est plus long pour le client, mais le marchand peut envoyer une réponse personnalisée au client.

  L'inconvénient du processus d'information en ligne après paiement est que le système du marchand risque d'être compromis en cas de demandes trop nombreuses envoyées à sa page d'après-paiement (par ex., un volume de transactions par minute important) – cela peut entraîner des temps de réponse longs avant que le client ne reçoive les informations à l'écran.

- En ligne mais passage par intervalles à une demande différée en cas d'échec des demandes en ligne :

  Cette option permet aux marchands qui ont besoin d'informations d'après-paiement en ligne (afin de personnaliser la réponse affichée au client) de disposer d'une option de repli en cas d'échec de la demande en ligne sur leur page d'après-paiement. Dans ce cas, nous effectuons un nouvel essai de demande d'informations toutes les dix minutes (maximum quatre fois) (différé). Cela permet au marchand d'éviter de passer à côté des informations de transaction en cas d'échec de la demande en ligne d'informations après-paiement en raison, par ex., de problèmes de serveur temporaires de son côté. Notre système affichera des informations standard sur la transaction pour le client (voir Réaction par défaut).

9.3.3 Réponse envoyée au client

Nous utilisons l'éventuelle réponse contenue sur votre page d'après-paiement pour afficher les informations (à la fin de la page de transaction) pour votre client.

Si votre page d'après-paiement répond au moyen : d'une page HTML (contenant une balise <html>) ou d'une redirection (HTTP 302 Object Moved), notre système envoie cette page HTML « telle quelle » au navigateur du client ou effectue la redirection, plutôt que de rediriger votre client au terme de votre processus d'informations après-paiement vers l'un des quatre URL que vous aurez éventuellement envoyés dans les champs masqués (accepturl, exceptionurl, cancelurl et declineurl , tels que décrits au chapitre Redirection en fonction du résultat du paiement).

Vous pouvez aussi, si vous n'utilisez aucune des options mentionnées plus haut pour communiquer les informations à votre client, programmer votre page d'après-paiement pour répondre par quelques lignes de texte (pas de balise <html>) que nous intégrerons dans notre réponse standard, ou notre système se contentera d'afficher la réponse standard (comme indiqué au chapitre Réaction par défaut).

9.4 Sécurité : vérification de l'origine de la requête

Lorsque notre système vous envoie une demande contenant des paramètres, vous avez deux moyens de vérifier que la demande émane effectivement de notre système : une vérification de l'adresse IP et une signature SHA.

9.4.1 Vérification de l'adresse IP (uniquement pour les demandes d'information)

Vous pouvez configurer nos adresses IP dans votre pare-feu pour vous assurer que la demande émane de l'un de nos serveurs ; vous pouvez aussi tout simplement vérifier l'origine IP dans vos CGI. Les adresses IP sont publiées dans la rubrique FAQ de votre compte. Veuillez noter qu'il existe différentes catégories d'adresses IP possibles et que ces adresses IP sont susceptibles de changer !

9.4.2 Signature SHA-OUT (pour les demandes d'information et les redirections)

Nous vous recommandons vivement d'utiliser une signature SHA pour vérifier le contenu des demandes ou les redirections ; cela empêchera par exemple les clients de toucher aux données dans le champ URL, ce qui pourrait entraîner une mise à jour erronée de la base de données. Pour de plus amples informations sur la signature SHA-OUT, veuillez vous reporter à l'Annexe: SHA.

9.5 E-mails de confirmation

9.5.1 E-mails envoyés au marchand

Notre système peut vous envoyer un e-mail de confirmation de paiement pour chaque transaction (une option à configurer sous l'onglet « E-mails de transaction », dans la rubrique « E-mails pour le marchand » sur la page d'information technique).

Vous pouvez aussi recevoir des e-mails vous informant des changements de statut des transactions.

9.5.2 E-mails envoyés au client

Notre système peut envoyer un courrier électronique automatique à votre client pour l'informer de l'enregistrement de la transaction. Il s'agit d'un message standard et vous ne pouvez pas en changer le contenu.

Vous pouvez activer cette option dans la section „E-mails pour le client“ de l'onglet „E-mails de transaction“ de la page Information Technique.

Vous pouvez également choisir d'envoyer au client un courriel lorsqu'une transaction est confirmée (capture de données) et remboursée en cochant les cases correspondantes. En tant qu'expéditeur (« From ») de ces courriels, vous pouvez configurer l'adresse électronique à utiliser dans les courrriels relatifs à la transaction (Adresse e-mail de support à insérer dans les e-mails relatifs aux transactions). Si vous n'indiquez pas d'adresse électronique ici, nous utiliserons la première adresse saisie sous "Adresse(s) e-mail pour les e-mails relatifs aux transactions" à la section "E-mails pour le marchand".

Pour pouvoir envoyer des courriels de confirmation à votre client, vous devez indiquer son adresse électronique dans le champ masqué :

```
<input type="hidden" name="EMAIL" value="">
```

Champ	Description
EMAIL	Adresse e-mail du client

Vous trouverez de plus amples informations sur ces champs dans votre compte PostFinance. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.

10 Autres champs masqués facultatifs

Il existe un certain nombre d'autres champs masqués facultatifs que le marchand peut nous envoyer à des fins bien précises. Dans le présent chapitre, nous donnons un aperçu de ces champs masqués et de leur objet.

10.1 Moyen de paiement et caractéristiques de la page de paiement

10.1.1 Choix du moyen de paiement du côté du marchand

10.1.1.1 Afficher un moyen de paiement déterminé

Lorsque notre page de paiement sécurisé s'affiche chez le client, on lui présente les moyens de paiement possibles que le marchand a activés sur son compte. Lorsque le client doit choisir son moyen de paiement sur le site du marchand et non sur notre page de paiement, celui-ci peut nous envoyer le nom du moyen de paiement et sa marque (uniquement lorsque le moyen de paiement est « CreditCard ») dans les champs masqués pour que nous n'affichions que ce moyen de paiement sur notre page de paiement et que nous n'acceptions que les paiements effectués par ce biais.

Ces champs masqués sont les suivants :

<input type="hidden" name="PM" value="">

<input type="hidden" name="BRAND" value="">

Champ	Objet
PM	Moyen de paiement
BRAND	Marque de la carte de crédit

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

Exemples

* Champs masqués dans l'hypothèse où votre client opte pour VISA sur votre site :

<input type="hidden" name="PM" value="CreditCard ">

<input type="hidden" name="BRAND" value="VISA">

* Champ masqués dans l'hypothèse où le seul moyen de paiement que vous acceptez dans ce cas est la carte de crédit (par exemple, si vous avez aussi d'autres moyens de paiement que vous ne souhaitez pas afficher) :

<input type="hidden" name="PM" value="CreditCard ">

<input type="hidden" name="BRAND" value="">

* Champs masqués dans l'hypothèse où votre client opte pour iDEAL sur votre site :

<input type="hidden" name="PM" value="iDEAL">

<input type="hidden" name="BRAND" value="">

10.1.1.2 Permettre au client de choisir un autre moyen de paiement : backurl

Lorsque le client choisit son moyen de paiement sur le site du marchand, nous n'affichons que le moyen de paiement sélectionné sur notre page de paiement.

Lorsque le paiement échoue avec ce moyen de paiement et que le client souhaite tenter de régler avec un autre moyen de paiement, la liste des moyens de paiement du marchand ne s'affiche pas

sur nos pages de paiement sécurisé étant donné que le choix du moyen de paiement a été opéré sur le site du marchand et non sur nos ages de paiement sécurisé.

Dans ce cas, le marchand peut utiliser le « backurl » pour rediriger le client vers un URL sur le site du marchand, où il va pouvoir choisir un autre moyen de paiement. Lorsque le client clique sur le bouton « Back » sur notre page de paiement sécurisé à la suite d'une autorisation refusée, ou après avoir annulé l'opération à partir d'un site tiers ou du site d'une banque, nous le redirigeons vers l'URL que le marchand a défini comme « backurl ».

IMPORTANT

Le bouton « back » dont nous parlons dans la présente section est le bouton « back » situé sur nos pages de paiement sécurisé, et NON le bouton « back » de votre navigateur.

Vous pouvez saisir le « backurl » sous l'onglet « Affichage de la page de paiement » sur la page d'information technique de votre compte, mais vous pouvez aussi nous envoyer un « backurl » bien précis dans les champs masqués pour une transaction si vous préférez éviter d'utiliser le même « backurl » que celui saisi sous l'onglet « Affichage de la page de paiement » de la page d'informations techniques de votre compte.

Le « backurl » envoyé dans les champs masqués l'emporte sur le « backurl » saisi sous l'onglet « Affichage de la page de paiement » de la page d'information technique de votre compte. Vous pouvez envoyer le « backurl » dans le champ masqué suivant :

```
<input type="hidden" name="backurl" value="">
```

Champ	Objet
backurl	URL de la page Web à afficher chez le client lorsqu'il clique sur le bouton « back » de notre page de paiement sécurisé.

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au Parameter Cookbook en ligne.

Lorsque le client choisit son moyen de paiement sur nos pages de paiement sécurisé et non sur le site du marchand, le « backurl » n'est pas pris en considération. Lorsque le client clique sur le bouton « back » sur notre page de paiement sécurisé, il est simplement redirigé vers notre page de sélection du moyen de paiement sécurisé, qui contient la liste des moyens de paiement acceptés par le marchand.

10.1.2 Afficher une liste déterminée de moyens de paiement

Lorsque le client doit choisir son moyen de paiement à partir d'une liste de moyens de paiement sur notre page de paiement, le marchand peut nous envoyer cette liste dans les champs masqués pour que nous n'affichions que ces moyens de paiement sur notre page de paiement.

Ce champ masqué est le suivant :

```
<input type="hidden" name="PMLIST" value="">
```

Champ	Objet
PMLIST	Liste des moyens de paiement et/ou des marques de cartes de crédit sélectionnés. Éléments séparés par un « ; » (point-virgule).

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

Exemples

* Champ masqué dans l'hypothèse où vous voulez que votre client choisisse entre VISA et iDEAL sur notre page de paiement (par ex., si vous proposez aussi d'autres moyens de paiement que vous ne souhaitez pas afficher) :

```
<input type="hidden" name="PMLIST" value="VISA;iDEAL">
```

10.1.3 Exclure une liste déterminée de moyens de paiement

Si le marchand ne souhaite pas présenter certaines marques spécifiques, cela peut être déterminé par un champ masqué.

Ceci est particulièrement pratique pour les Sub-Brands, quand un marchand veut accepter une marque (ex: MasterCard) mais pas la sous-marque (ex: Maestro)

Le champ masqué est le suivant:

<input type="hidden" name="EXCLPMLIST" value="">

Champ	Objet
EXCLPMLIST	Liste des moyens de paiement et/ou des marques de cartes de crédit à exclure. Éléments séparés par un « ; » (point-virgule).

Pour des informations techniques complémentaires sur ces champs, veuillez vous reporter au Parameter Cookbook en ligne.

10.1.4 Présentation des moyens de paiement

Vous pouvez définir la présentation/liste des moyens de paiement sur notre page de paiement au moyen du champ masqué suivant :

<input type="hidden" name="PMLISTTYPE" value="">

Champ	Valeurs possibles
PMLISTTYPE	Les valeurs possibles sont 0, 1 et 2. 0 : Logos regroupés horizontalement avec le nom du groupe sur la gauche (valeur par défaut) 1 : Logos regroupés horizontalement sans les noms des groupes 2 : Liste verticale de logos avec moyen de paiement et nom de la marque

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au Parameter Cookbook en ligne.

10.1.5 3-D secure

Si vous travaillez avec 3-D Secure, vous pouvez définir la façon dont vous souhaitez que la page d'identification s'affiche chez le client en nous envoyant un paramètre supplémentaire dans les champs masqués.

IMPORTANT

Veuillez noter que pour certaines méthodes de paiement (Visa, MasterCard, JCB, ...) , la valeur 'POPUP' n'est pas autorisée et sera convertie en 'MAINW' par le système. Nous vous conseillons de tester le comportement de ce paramètre pour chaque méthode de paiement.

Ce champ masqué est le suivant :

<input type="hidden" name="WIN3DS" value="">

Champ	Valeurs possibles
WIN3DS	« MAINW » : pour afficher la page d'identification dans la fenêtre principale (valeur par défaut) « POPUP » : pour afficher la page d'identification dans une fenêtre contextuelle (pop-up) et revenir à la fenêtre principale à la fin

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au

Parameter Cookbook en ligne.

10.1.6 Subdivision en cartes de crédit/débit

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

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

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

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

Si le paiement est traité avec succès avec le paramètre CREDITDEBIT, ce même paramètre est également renvoyé dans le retour d'information post-vente. Cependant, si les valeurs soumises sont C ou D, les valeurs de retour sont « CREDIT » ou « DEBIT ».

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

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

10.2 Code Opération

IMPORTANT

La possibilité de travailler en deux étapes (autorisation + saisie de données) varie selon les moyens de paiement que vous souhaitez utiliser. (Voir l'aperçu en ligne Payment Methods Processing/Procedure)

Vous pouvez nous envoyer un code d'opération déterminé pour une transaction si vous préférez utiliser un code d'opération autre que celui sélectionné sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Code d'opération par défaut » de la page d'information technique de votre compte pour cette transaction.

Le code d'opération que vous nous envoyez dans les champs masqués l'emporte sur le code d'opération général sélectionné sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Code d'opération par défaut » de la page d'information technique de votre compte. Vous pouvez envoyer le code d'opération dans le champ masqué suivant :

<input type="hidden" name="OPERATION" value="">

Champ	Objet
OPERATION	Code d'opération pour la transaction. Valeurs possibles pour les nouvelles commandes : ▪ RES : demande d'autorisation

Champ	Objet
	▪ SAL : demande de vente (paiement)

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au Parameter Cookbook en ligne.

IMPORTANT

Afin que ce parametre soit pris en compte par notre système, n'oubliez pas de l'inclure dans la signature SHA pour la transaction. Pour plus d'infos sur SHA, veuillez vous reporter à l'Annexe: SHA

10.3 Champ Utilisateur

Si vous avez plusieurs utilisateurs dans votre compte et que vous souhaitez enregistrer les transactions liées à un utilisateur particulier (par ex., pour les agents de centres d'appels qui enregistrent des transactions via e-Commerce), vous pouvez envoyer l'UserID dans le champ masqué suivant :

<input type="hidden" name="USERID" value="">

Champ	Objet
USERID	Le nom d'utilisateur défini sur la page de gestion de l'utilisateur du compte

Pour des informations techniques complémentaires sur ce champ, veuillez vous reporter au Parameter Cookbook en ligne.

Ce champ n'est qu'informatif, puisqu'il sert à ajouter un UserID pour une transaction déterminée. Nous n'effectuons aucune vérification de notre côté pour établir, par ex., s'il y a eu des erreurs de mot de passe pour cet utilisateur. La seule vérification que nous effectuons concerne la validité de l'UserID. Si l'UserID n'existe pas, nous le remplaçons par l'UserID par défaut du compte (PSPID).

Veuillez vous reporter au Parameter Cookbook en ligne pour d'autres champs.

10.4 Informations de livraison et de facturation

Certains modes de paiement peuvent exiger que vous fournissiez des informations sur la livraison. Pour ce faire, vous pouvez utiliser les champs suivants :

Champ	Type/ longueur	Utilisation
ORDERSHIPMETH	AN (25)	Mode de livraison
ORDERSHIPCOST	N	Frais de livraison
ORDERSHIPTAXCODE	N	Code taxe de livraison
CUID	AN (50)	Numéro de sécurité sociale / numéro d'enregistrement de la société
CIVILITY	AN (10)	Titre (M., Mme, Dr, etc.) - adresse de facturation
ECOM_BILLTO_POSTAL_NAME_FIRST	AN (35)	Prénom - adresse de facturation
ECOM_BILLTO_POSTAL_NAME_LAST	AN (35)	Nom - adresse de facturation

Champ	Type/ longueur	Utilisation
ECOM_BILLTO_POSTAL_ STREET_LINE1	AN (35)	Rue - adresse de facturation
ECOM_BILLTO_POSTAL_ STREET_NUMBER	AN (10)	Numéro - adresse de facturation
ECOM_BILLTO_POSTAL_ POSTALCODE	AN (10)	Code postal - adresse de facturation
ECOM_BILLTO_POSTAL_CITY	AN (40)	Ville - adresse de facturation
ECOM_BILLTO_POSTAL_ COUNTRYCODE	AN (2)	Code pays (BE, FR, NL, DE, etc.) - adresse de facturation
ECOM_SHIPTO_POSTAL_NAME _PREFIX	AN (10)	Titre (M., Mme, etc.) - adresse de livraison
ECOM_SHIPTO_POSTAL_NAME _FIRST	AN (35)	Prénom - adresse de livraison
ECOM_SHIPTO_POSTAL_NAME _LAST	AN (35)	Nom - adresse de livraison
ECOM_SHIPTO_POSTAL_STATE	AN (2)	Code État des États-Unis (code ISO *) - adresse de livraison
ECOM_SHIPTO_POSTAL_ STREET_LINE1	AN (35)	Rue - adresse de livraison
ECOM_SHIPTO_POSTAL_ STREET_NUMBER	AN (10)	Numéro - adresse de livraison
ECOM_SHIPTO_POSTAL_ POSTALCODE	AN (10)	Code postal - adresse de livraison
ECOM_SHIPTO_POSTAL_CITY	AN (25)	Ville - adresse de livraison
ECOM_SHIPTO_POSTAL_ COUNTRYCODE	AN (2)	Code pays - adresse de livraison
ECOM_SHIPTO_ONLINE_EMAIL	AN (50)	Adresse électronique - adresse de livraison
ECOM_SHIPTO_DOB	aaaa-MM-jj	Date de naissance

(Les codes ISO des États d'Amérique se trouvent ici. Exemple : AL (Alabama), FL (Floride))*

Vous trouverez de plus amples détails sur ces champs dans notre Livre des paramètres en ligne.

10.5 Détails de la commande

Certains modes de paiement peuvent exiger que vous fournissiez des informations détaillées sur la commande. Pour ce faire, vous pouvez utiliser les champs suivants :

Champ	Type/ longueur	Utilisation
ITEMIDX	Alphanum (15)	Identification de l'article (remplacer X par un nombre pour envoyer plusieurs exemplaires de l'article : ITEMID1, ITEMID2, etc.)

Champ	Type / longueur	Utilisation
ITEMNAMEX	Alphanum (50)	Désignation de l'article (remplacer X par un nombre pour envoyer plusieurs exemplaires de l'article : ITEMNAME1, ITEMNAME2, etc.)
ITEMPRICEX	Numérique	Prix de l'article (remplacer X par un nombre pour envoyer plusieurs exemplaires de l'article : ITEMPRICE1, ITEMPRICE2, etc.)
ITEMQUANTX	Numérique	Quantité de l'article (remplacer X par un nombre pour envoyer plusieurs exemplaires de l'article : ITEMQUANT1, ITEMQUANT2, etc.)
ITEMVATCODEX	Numérique	Code TVA de l'article (remplacer X par un nombre pour envoyer plusieurs exemplaires de l'article : ITEMVATCODE1, ITEMVATCODE2, etc.)

Vous trouverez de plus amples détails sur ces champs dans notre Livre des paramètres en ligne.

10.6 Direct Debits

Enter topic text here.

10.6.1 Direct Debits DE (ELV)

Les champs suivants peuvent être envoyés avec les transactions de prélèvement automatique DE (ELV). Ils seront affichés à l'intention du client dans le texte Mandate (Mandat), sur la page de paiement.

Champ	Description
CN	Nom du titulaire de la carte
Facultativement pour les transactions SEPA (*) (sans objet pour les moyens de paiement Billpay et Wirecard) :	
MANDATEID	Référence unique du mandat Max. 35 caractères alphanumériques (AN), jeu de caractères : « A-Z a-z 0-9 espace /-?:().,'+ »

Vous trouverez de plus amples détails sur ces champs dans notre Parameter Cookbook en ligne.

Remarque : Ces champs peuvent être renvoyés dans le retour postpaiement (paramètres de commerce électronique dynamiques) et doivent être inclus dans le calcul SHA-IN (et, le cas échéant, SHA-OUT).

Remarques concernant SEPA (*)

- Si vous ne définissez pas le champ CN, il reste vide sur la page de paiement.
- Si vous ne fournissez pas de valeur pour le champ MANDATEID, nous utilisons la valeur du champ ORDERID. Cependant, si la valeur ORDERID n'est pas conforme aux spécifications du champ MANDATEID, c'est le code PAYID qui est utilisé.
- Si vous n'avez pas activé le mode SEPA dans la page de configuration des prélèvements automatiques DE / ELV, votre acquéreur génère une référence MANDATEID.

Les champs présentés à l'acheteur sont les suivants :

- IBAN
- Bankkonto (Compte bancaire)

- BLZ (Code banque)

L'acheteur peut choisir de saisir l'IBAN ou la combinaison numéro de compte bancaire et code d'identification de la banque. Si ces deux options sont complétées, c'est l'IBAN qui est pris en considération.

*(*SEPA : Single Euro Payments Area, c'est l'espace unique de paiements en euros de l'UE)*

10.6.2 Direct Debits NL

Les champs suivants doivent être envoyés avec les transactions de prélèvement automatique NL (uniquement via Equens) :

Champ	Description
MANDATEID	Référence unique du mandat (pour les paiements SEPA*) Max. 35 caractères alphanumériques (AN), jeu de caractères : « A-Z a-z 0-9 /-?:().,'+ » *Ce champ s'applique uniquement aux transactions SEPA (*). S'il n'est pas défini, c'est la valeur ORDERID qui est adoptée.*
SIGNDATE	Date à laquelle le mandat a été signé par l'acheteur. Format : AAAAMMJJ *Ce champ s'applique uniquement aux transactions SEPA (*). S'il n'est pas défini, c'est la date de la transaction qui est adoptée.*
SEQUENCETYPE	Valeurs possibles pour indiquer une transaction de type prélèvement automatique (max. 4 caractères alphanumériques) : - « FRST » : Premier ensemble d'une série d'instructions de prélèvement automatique - « RCUR » : Instructions de prélèvement automatique dans lesquelles l'autorisation du débiteur est utilisée pour les transactions de prélèvement automatique lancées par le créancier - « FNAL » : Dernier ensemble d'une série d'instructions de prélèvement automatique (après celui-ci, il n'est plus possible d'utiliser le même MandateID) - « OOFF » : Instruction de prélèvement automatique dans laquelle l'autorisation du débiteur est utilisée pour lancer une transaction de prélèvement automatique unique *Ce champ s'applique uniquement aux transactions SEPA (*).* *S'il n'est pas défini, la transaction est considérée comme unique (« one-off » ou « OOFF »).* *Si « FRST », « RCUR » ou « FNAL » est envoyé, vous devez soumettre les valeurs en combinaison avec les champs MANDATEID et SIGNDATE.*

Vous trouverez de plus amples détails sur ces champs dans notre Parameter Cookbook en ligne.

Remarque : Ces champs peuvent être renvoyés dans le retour postpaiement (paramètres de commerce électronique dynamiques) et doivent être inclus dans le calcul SHA-IN (et, le cas échéant, SHA-OUT).

(Single Euro Payments Area, c'est l'espace unique de paiements en euros de l'UE)*

Les champs présentés à l'acheteur sur la page de paiement sont les suivants :

- IBAN

11 Annexe: SHA

Pour chaque commande, le serveur du marchand génère une chaîne de caractères unique, hachée au moyen de l'algorithme SHA-1 développé par NIST (voir ici).

11.1 Signature SHA-IN

La chaîne est créée en concaténant les valeurs des champs envoyés avec la commande (triés par ordre alphabétique, dans le format 'paramètre =valeur'), séparés par une clé. Cette clé est définie dans les Informations Techniques du commerçant, sous l'onglet "Contrôle de données et d'Origine", section "Contrôles pour e-Commerce" Pour obtenir la liste complète des paramètres à inclure dans la chaîne SHA, veuillez vous reporter à l'Annexe 6. Veuillez observer que ces valeurs sont sensibles à la casse lors de leur compilation pour former la chaîne avant le hachage !

IMPORTANT

- Tous les paramètres que vous envoyez (et qui apparaissent dans la liste dans Annexe: Paramètres à inclure dans le calcul SHA), seront inclus dans la chaîne.
- Tous les noms de paramètres doivent être en MAJUSCULES (pour éviter toute confusion)
- Tous les paramètres doivent être classés en ordre alphabétique
- Les paramètres qui n'ont pas de valeur ne doivent PAS être inclus dans la chaîne
- Notez que certains algorithmes de tri placent les caractères spéciaux devant la première lettre de l'alphabet, d'autres à la fin. En cas de doute, veuillez respecter l'ordre tel qu'indiqué dans la liste SHA.
- Lorsque vous souhaitez transférer votre compte de Test vers l'environnement de production en utilisant le lien disponible dans le back-office, une signature SHA-IN aléatoire sera automatiquement configurée dans votre compte de production
- Pour plus de sécurité, nous vous demandons d'utiliser des mots de passe SHA différents pour TEST et PROD. Remarquez que s'ils sont identiques, votre mot de passe TEST sera modifié par notre système (vous en serez évidemment averti)

Lorsque vous hachez la chaîne compilée avec l'algorithme SHA, le système générera un condensé hexadécimal. La longueur de ce condensé SHA est de 40 caractères pour le SHA-1, de 64 pour le SHA-256 et de 128 pour le SHA-512. Ce résultat devrait être envoyé à notre système dans votre commande, en utilisant le champ « SHASIGN ».

Notre système recomposera la chaîne SHA en fonction des paramètres reçus et comparera le condensé du commerçant avec le condensé que nous aurons généré. Si le résultat n'est pas identique, la commande sera refusée. Cette vérification garantit l'exactitude et l'intégrité des données de la commande.

Vous pouvez tester votre SHASign à l'adresse https://e-payment.postfinance.ch/ncol/test/testsha.asp

Exemple d'un calcul SHA-1-IN élémentaire

Paramètres (en ordre alphabétique)
AMOUNT: 15.00 -> 1500
CURRENCY: EUR
LANGUAGE: en_US
ORDERID: 1234
PSPID: MyPSPID

Clé SHA
Mysecretsig1875!?

Chaîne à hacher
AMOUNT=1500Mysecretsig1875!?CURRENCY=EURMysecretsig1875!?
LANGUAGE=en_USMysecretsig1875!?ORDERID=1234Mysecretsig1875!?

PSPID=MyPSPIDMysecretsig1875!?

Condensé obtenu
F4CC376CD7A834D997B91598FA747825A238BE0A (SHA-1)
E019359BAA3456AE5A986B6AABD22CF1B3E09438739E97F17A7F61DF5A11B30F (SHA-256)
D1CFE8833A297D0922E908B2B44934B09EE966EF1584DC0D696304E07BB58BA71973C2383C831D878D8A243BB7D7DFFFBE53CEE21955CDFEF44FE82E551F859D (SHA-512)

Si le SHASign envoyé dans les champs cachés HTML de la transaction ne correspond pas au SHASign assemblé de notre côté avec les détails de la commande et la chaîne supplémentaire (mot de passe/ phrase secrète) entrée dans le champ „Signature SHA-1-IN“ dans la section „Contrôles pour e-Commerce“ de l'onglet „Contrôle des données et d'origine“ de la page Information Technique, vous recevrez le message d'erreur « unknown order/1/s».

Si rien n'est envoyé dans le champ « SHASign » des champs cachés HTML, même si une chaîne supplémentaire (mot de passe/phrase secrète) a été entrée dans le champ „Signature SHA-1-IN“ dans la section „Contrôles pour e-Commerce“ de l'onglet „Contrôle des données et d'origine“ de la page Information Technique – indiquant que vous voulez utiliser une signature SHA avec chaque transaction – vous recevrez un message d'erreur « unknown order/0/s».

Le champ masqué utilisé pour transmettre la signature SHA à notre système est le suivant :

Champ	Objet
SHASIGN	Chaîne de caractères unique pour la validation des données de commande Une chaîne hachée par l'algorithme SHA-1 contiendra toujours 40 caractères.

11.2 Signature SHA-OUT

La chaîne est créée en concaténant les valeurs des champs envoyés avec la commande (triés par ordre alphabétique, dans le format 'paramètre =valeur'), séparés par une clé. Cette clé est définie dans les Informations Techniques du commerçant, sous l'onglet "Contrôle de données et d'Origine", section "Contrôles pour e-Commerce" Pour obtenir la liste complète des paramètres à inclure dans la chaîne SHA, veuillez vous reporter à l'Annexe 6. Veuillez observer que ces valeurs sont sensibles à la casse lors de leur compilation pour former la chaîne avant le hachage !

IMPORTANT

- Tous les paramètres envoyés (et qui apparaissent dans la liste dans Annexe: Paramètres à inclure dans le calcul SHA), seront inclus dans la chaîne.
- Tous les paramètres doivent être classés en ordre alphabétique
- Les paramètres qui n'ont pas de valeur ne doivent PAS être inclus dans la chaîne
- Lorsque vous souhaitez transférer votre compte de Test vers l'environnement de production en utilisant le lien disponible dans le back-office, une signature SHA-OUT aléatoire sera automatiquement configurée dans votre compte de production
- Même si certains paramètres sont (partiellement) envoyés en minuscules par notre système, lors du calcul du SHA-OUT tous les paramètres doivent être mis en majuscules.
- Pour plus de sécurité, nous vous demandons d'utiliser des mots de passe SHA différents pour TEST et PROD. Remarquez que s'ils sont identiques, votre mot de passe TEST sera modifié par notre système (vous en serez évidemment averti)

Le marchand doit vérifier, de la même manière que nous le faisons pour SHA-IN, si la chaîne reçue correspond bien à la chaîne générée. Ceci permet de garantir l'intégrité des données.

Exemple de calcul SHA-OUT

Paramètres (en ordre alphabétique) :
ACCEPTANCE: 1234
amount: 15
BRAND: VISA

CARDNO: XXXXXXXXXXXX1111
currency: EUR
NCERROR: 0
orderID: 12
PAYID: 32100123
PM: CreditCard
STATUS: 9

Clé SHA (dans Information technique) :
Mysecretsig1875!?

Chaîne à hacher :
ACCEPTANCE=1234Mysecretsig1875!?AMOUNT=15Mysecretsig1875!?
BRAND=VISAMysecretsig1875!?CARDNO=XXXXXXXXXXXX1111Mysecretsig1875!?
CURRENCY=EURMysecretsig1875!?NCERROR=0Mysecretsig1875!?ORDERID=12Mysecretsig1875!?
PAYID=32100123Mysecretsig1875!?PM=CreditCardMysecretsig1875!?STATUS=9Mysecretsig1875!?

Condensé obtenu (SHA-1) :
209113288F93A9AB8E474EA78D899AFDBB874355

11.3 Module SHA

Pour pouvoir hacher une chaîne et nous l'envoyer, vous devez préalablement installer un modèle SHA sur votre serveur.

Vous pouvez trouver des modules SHA-1, SHA-256 et SHA-512 sur l'Internet ; vous ne devriez donc pas avoir de mal à en trouver un qui convienne à votre serveur. Pour vous aider à trouver un module SHA-1 adapté à votre environnement, nous avons dressé la liste de sites suivante :

Informations générales sur SHA sur W3.org :
http://www.w3.org/PICS/DSig/SHA1_1_0.html

.NET / SHA1 :
http://msdn.microsoft.com/fr-fr/library/system.security.cryptography.sha1.aspx

PHP / SHA1 :
http://www.php.net/manual/en/ref.mhash.php

12 Annexe: UTF-8

Par défaut, PostFinance utilise le codage de caractères ISO. Cependant, notre système supporte l'utilisation de l'UTF-8, pour autant que le marchand appelle les pages appropriées.

Pour e-Commerce, la page de paiement est https://e-payment.postfinance.ch/ncol/test/orderstandard_utf8.asp

IMPORTANT

- Notre système ne sait pas dynamiquement détecter le codage; le marchand a la responsabilité d'appeler la page appropriée;
- Si le marchand appelle la page de paiement UTF-8, l'encodage SHA se fera sur base de la chaine à encoder en UTF-8 également, aussi bien en SHA-IN qu'en SHA-OUT. Il existe une page de test SHA UTF-8 ici: https://e-payment.postfinance.ch/ncol/test/testsha_utf8.asp
- Si le marchand utilise des Templates dynamiques, assurez-vous que le codage UTF-8 soit déclaré dans le header html.

Notez que l'utilisation d'UTF-8 est obligatoire pour les langues suivantes:

- Arabe
- Coréen
- Grec
- Hébreu
- Japonais
- Russe
- Turc

13 Annexe: Dépannage

Cette rubrique contient une liste non exhaustive des erreurs possibles :

- *unknown order/1/r*
  Cette erreur signifie que le référant que nous avons détecté n'est pas un URL que le marchand a saisi dans le champ URL sous l'onglet « Contrôle de données et d'origine », dans la rubrique « Contrôles pour e-Commerce » de sa page d'information technique. Le marchand nous envoie le formulaire avec des champs masqués contenant les informations de commande d'une autre page que celle(s) saisie dans le champ URL sous l'onglet « Contrôle de données et d'origine », dans la rubrique « Contrôles pour e-Commerce ».
- *unknown order/0/r*
  Cette erreur signifie que notre serveur n'a pas détecté de référant dans la demande que nous avons reçue. Le marchand nous envoie des informations sur une commande, mais nous ignorons d'où elles proviennent. Assurez-vous que vous n'utilisez aucune méthode qui bloque les informations sur le référant (page de paiement en fenêtre contextuelle, configuration particulière du serveur Web, configuration du navigateur du client, ...). Lorsque le navigateur du client n'envoie pas les informations sur le référant, nous pouvons contourner la vérification du référant lorsqu'une SHASign est présente et correcte. (Voir chapitre 6.2)
- *unknown order/1/s*
  Vous recevez ce message d'erreur lorsque la SHASign envoyée dans les champs HTML masqués pour la transaction ne correspond pas à la SHASign calculée de notre côté sur la base des informations de la commande et de la chaîne supplémentaire (mot de passe/ phrase) saisie dans le champ « Signature SHA-IN » sous l'onglet « Contrôle de données et d'origine », dans la rubrique « Contrôles pour e-Commerce » de la page d'information technique.
- *unknown order/0/s*
  Vous recevez ce message d'erreur lorsque le champ « SHASign » contenu dans les champs HTML masqués est vide mais qu'une clé SHA a été saisie dans le champ Signature SHA-IN sous l'onglet « Contrôle de données et d'origine », dans la rubrique « Contrôles pour e-Commerce » de la page d'information technique pour indiquer que vous souhaitez utiliser une signature SHA pour chaque transaction.
- *PSPID not found or not active*
  Ce message indique que la valeur que vous avez saisie dans le champ PSPID n'existe pas dans l'environnement (test ou prod) concerné ou que le compte n'a pas encore été activé.
- *no <parameter> (par exemple : no PSPID)*
  Cette erreur signifie que la valeur que vous avez envoyée pour le champ obligatoire <parameter> est vide.
- *<parameter> too long (par exemple : currency too long)*
  Ce message d'erreur signifie que la valeur indiquée dans votre champ <parameter> dépasse la longueur maximale.
- *amount too long or not numeric: ... OU Amount not a number*
  Cette erreur signifie que le montant que vous avez envoyé dans les champs masqués dépasse la longueur maximale ou contient des caractères non valides, comme '.' ou '**,**' par exemple.
- *not a valid currency : ...*
  Cette erreur signifie que vous avez envoyé une transaction avec un code devise incorrect ou qui n'existe pas.
- *The currency is not accepted by the merchant*
  Cette erreur signifie que vous avez envoyé une transaction dans une devise qui n'a pas été enregistrée dans les informations de votre compte.
- *ERROR, PAYMENT METHOD NOT FOUND FOR : ...*
  Cette erreur signifie que la valeur PM que vous avez envoyée dans les champs masqués ne correspond à aucun des moyens de paiement que vous avez sélectionnés dans votre compte, ou que le moyen de paiement n'a pas été activé sur la page reprenant vos moyens de paiement.

14 Annexe: Bref aperçu des statuts

Cette rubrique contient une liste non exhaustive des statuts ; pour une liste complète, veuillez vous reporter à "La signification des statuts des paiements et des codes d'erreur éventuels" dans le menu Support de votre compte PostFinance.

Statut	NCERROR	NCSTATUS	Explication
5 Authorized	0	0	L'autorisation a été acceptée. Les codes d'autorisation sont disponibles dans le champ « ACCEPTANCE ». Le statut sera 5 si vous avez opté pour le code d'opération par défaut « Autorisation » sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Code d'opération par défaut » de la page d'information technique de votre compte.
9 Payment requested	0	0	Le paiement a été accepté. Les codes d'autorisation sont disponibles dans le champ « ACCEPTANCE ». Le statut initial de la transaction sera 9 si vous avez opté pour le code d'opération par défaut « Sale » sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Code d'opération par défaut » de la page d'information technique de votre compte.
0 Invalid or incomplete	500....	5	Un des champs des données de paiement au moins est invalide ou manquant. Les champs NCERROR et NCERRORPLUS donnent une explication de l'erreur.
2 Authorization refused	300....	3	L'autorisation a été refusée par l'établissement financier. Le client peut effectuer une nouvelle tentative d'autorisation après avoir sélectionné une autre carte ou un autre moyen de paiement.
51 Authorization waiting	0	0	L'autorisation va être traitée hors-ligne. Il s'agit de la réponse standard lorsque le marchand a opté pour le traitement hors-ligne dans la configuration de son compte. Le statut sera 51 dans deux cas : • Si vous avez défini « Always offline (Scheduled) » pour le traitement des paiements sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Traitement des transactions individuelles » de la page d'information technique de votre compte. • Lorsque le système en ligne de l'acquéreur est indisponible et que vous avez défini « Online mais basculer en offline durant les périodes d'indisponibilité du système acquéreur » pour traiter les paiements sous l'onglet « Paramètres de transaction globaux », dans la rubrique « Traitement des transactions individuelles » de la page d'information technique de votre compte.
91 Payment processing	0	0	La saisie de données sera traitée hors-ligne.
52 Authorization not known	200...	2	Un problème technique est survenu durant le processus d'autorisation/paiement, ce qui donne un

Statut	NCERROR	NCSTATUS	Explication
ou 92 Payment uncertain			résultat imprévisible. Le marchand peut contacter le *helpdesk* de l'acquéreur pour connaître le statut exact du paiement ou il peut attendre la mise à jour du statut dans notre système. Le client ne doit pas effectuer de nouvelle tentative d'autorisation étant donné que l'autorisation/le paiement ont peut-être déjà été acceptés.
93 Payment refused	300....	3	Un problème technique est survenu.

15 Annexe: e-Commerce par e-mail

Vous pouvez envoyer à vos clients une demande de paiement par e-mail pour rediriger le client vers notre page de paiement sécurisé via un bouton ou un lien dans l'e-mail.

Lorsque l'e-mail est au format HTML, vous pouvez utiliser un formulaire contenant des champs HTML masqués pour nous envoyer les paramètres nécessaires au format POST.

Lorsque l'e-mail est au format texte brut, vous pouvez ajouter les paramètres nécessaires à l'URL au format GET. (par ex., https://e-payment.postfinance.ch/ncol/test/orderstandard.asp?PSPID=TESTSTD&orderID=order123&amount=12500&currency=EUR&SHASIGN=8DDF4795640EB9FE9B367315C48E47338129A4F5& …)

Veuillez vous reporter au chapitre Lien entre le site Web du marchand et notre page de paiement pour de plus amples informations.

IMPORTANT

Pour que e-Commerce par e-mail fonctionne, soyez attentif aux aspects suivants liés à la vérification avant le paiement :

- Le champ référant/URL doit rester vide dans le champ URL « Contrôle de données et d'origine », dans la rubrique « Contrôles pour e-Commerce » de la page d'information technique de votre compte afin d'éviter les erreurs « unknown order/1/r ».
- Vous devez utiliser une signature SHA en guise de méthode de vérification de données pour les informations sur la commande. Pour de plus amples informations sur la signature SHA-1-IN, veuillez vous reporter à l'Annexe: SHA.

16 Annexe: Liste des paramètres à inclure dans les signatures SHA

16.1 SHA-IN

ACCEPTANCE
ACCEPTURL
ADDMATCH
ADDRMATCH
AIACTIONNUMBER
AIAGIATA
AIAIRNAME
AIAIRTAX
AIBOOKIND*XX*
AICARRIER*XX*
AICHDET
AICLASS*XX*
AICONJTI
AIDEPTCODE
AIDESTCITY*XX*
AIDESTCITYL*XX*
AIEXTRAPASNAME*XX*
AIEYCD
AIFLDATE*XX*
AIFLNUM*XX*
AIGLNUM
AIINVOICE
AIIRST
AIORCITY*XX*
AIORCITYL*XX*
AIPASNAME
AIPROJNUM
AISTOPOV*XX*
AITIDATE
AITINUM
AITINUML*XX*
AITYPCH
AIVATAMNT
AIVATAPPL
ALIAS
ALIASOPERATION
ALIASPERSISTEDAFTERUSE
ALIASUSAGE
ALLOWCORRECTION
AMOUNT
AMOUNT*XX*

AMOUNTHTVA
AMOUNTTVA
ARP_TRN
BACKURL
BATCHID
BGCOLOR
BLVERNUM
BIC
BIN
BRAND
BRANDVISUAL
BUTTONBGCOLOR
BUTTONTXTCOLOR
CANCELURL
CARDNO
CATALOGURL
CAVV_3D
CAVVALGORITHM_3D
CERTID
CHECK_AAV
CIVILITY
CN
COM
COMPLUS
CONVCCY
COSTCENTER
COSTCODE
CREDITCODE
CREDITDEBIT
CUID
CURRENCY
CVC
CVCFLAG
DATA
DATATYPE
DATEIN
DATEOUT
DBXML
DCC_COMMPERC
DCC_CONVAMOUNT
DCC_CONVCCY
DCC_EXCHRATE
DCC_EXCHRATETS
DCC_INDICATOR
DCC_MARGINPERC
DCC_REF
DCC_SOURCE
DCC_VALID

DECLINEURL
DELIVERYDATE
DEVICE
DISCOUNTRATE
DISPLAYMODE
ECI
ECI_3D
ECOM_BILLTO_COMPANY
ECOM_BILLTO_POSTAL_CITY
ECOM_BILLTO_POSTAL_COUNTRYCODE
ECOM_BILLTO_POSTAL_COUNTY
ECOM_BILLTO_POSTAL_NAME_FIRST
ECOM_BILLTO_POSTAL_NAME_LAST
ECOM_BILLTO_POSTAL_NAME_PREFIX
ECOM_BILLTO_POSTAL_POSTALCODE
ECOM_BILLTO_POSTAL_STREET_LINE1
ECOM_BILLTO_POSTAL_STREET_LINE2
ECOM_BILLTO_POSTAL_STREET_LINE3
ECOM_BILLTO_POSTAL_STREET_NUMBER
ECOM_BILLTO_TELECOM_MOBILE_NUMBER
ECOM_BILLTO_TELECOM_PHONE_NUMBER
ECOM_CONSUMERID
ECOM_CONSUMER_GENDER
ECOM_CONSUMEROGID
ECOM_CONSUMERORDERID
ECOM_CONSUMERUSERALIAS
ECOM_CONSUMERUSERPWD
ECOM_CONSUMERUSERID
ECOM_ESTIMATEDDELIVERYDATE
ECOM_ESTIMATEDELIVERYDATE
ECOM_PAYMENT_CARD_EXPDATE_MONTH
ECOM_PAYMENT_CARD_EXPDATE_YEAR
ECOM_PAYMENT_CARD_NAME
ECOM_PAYMENT_CARD_VERIFICATION
ECOM_SHIPMETHOD
ECOM_SHIPMETHODDETAILS
ECOM_SHIPMETHODSPEED
ECOM_SHIPMETHODTYPE
ECOM_SHIPTO_COMPANY
ECOM_SHIPTO_DOB
ECOM_SHIPTO_ONLINE_EMAIL
ECOM_SHIPTO_POSTAL_CITY
ECOM_SHIPTO_POSTAL_COUNTRYCODE
ECOM_SHIPTO_POSTAL_COUNTY
ECOM_SHIPTO_POSTAL_NAME_FIRST
ECOM_SHIPTO_POSTAL_NAME_LAST
ECOM_SHIPTO_POSTAL_NAME_PREFIX
ECOM_SHIPTO_POSTAL_POSTALCODE

ECOM_SHIPTO_POSTAL_STATE
ECOM_SHIPTO_POSTAL_STREET_LINE1
ECOM_SHIPTO_POSTAL_STREET_LINE2
ECOM_SHIPTO_POSTAL_STREET_NUMBER
ECOM_SHIPTO_TELECOM_FAX_NUMBER
ECOM_SHIPTO_TELECOM_MOBILE_NUMBER
ECOM_SHIPTO_TELECOM_PHONE_NUMBER
ECOM_SHIPTO_TVA
ED
EMAIL
EXCEPTIONURL
EXCLPMLIST
EXECUTIONDATE*XX*
FACEXCL*XX*
FACTOTAL*XX*
FIRSTCALL
FLAG3D
FONTTYPE
FORCECODE1
FORCECODE2
FORCECODEHASH
FORCEPROCESS
FORCETP
FP_ACTIV
GENERIC_BL
GIROPAY_ACCOUNT_NUMBER
GIROPAY_BLZ
GIROPAY_OWNER_NAME
GLOBORDERID
GUID
HDFONTTYPE
HDTBLBGCOLOR
HDTBLTXTCOLOR
HEIGHTFRAME
HOMEURL
HTTP_ACCEPT
HTTP_USER_AGENT
INCLUDE_BIN
INCLUDE_COUNTRIES
INITIAL_REC_TRN
INVDATE
INVDISCOUNT
INVLEVEL
INVORDERID
ISSUERID
IST_MOBILE
ITEM_COUNT
ITEMATTRIBUTES*XX*

ITEMCATEGORY*XX*
ITEMCOMMENTS*XX*
ITEMDESC*XX*
ITEMDISCOUNT*XX*
ITEMFDMPRODUCTCATEG*XX*
ITEMID*XX*
ITEMNAME*XX*
ITEMPRICE*XX*
ITEMQUANT*XX*
ITEMQUANTORIG*XX*
ITEMUNITOFMEASURE*XX*
ITEMVAT*XX*
ITEMVATCODE*XX*
ITEMWEIGHT*XX*
LANGUAGE
LEVEL1AUTHCPC
LIDEXCL*XX*
LIMITCLIENTSCRIPTUSAGE
LINE_REF
LINE_REF1
LINE_REF2
LINE_REF3
LINE_REF4
LINE_REF5
LINE_REF6
LIST_BIN
LIST_COUNTRIES
LOGO
MANDATEID
MAXITEMQUANT*XX*
MERCHANTID
MODE
MTIME
MVER
NETAMOUNT
OPERATION
ORDERID
ORDERSHIPCOST
ORDERSHIPMETH
ORDERSHIPTAX
ORDERSHIPTAXCODE
ORIG
OR_INVORDERID
OR_ORDERID
OWNERADDRESS
OWNERADDRESS2
OWNERCTY
OWNERTELNO

OWNERTELNO2
OWNERTOWN
OWNERZIP
PAIDAMOUNT
PARAMPLUS
PARAMVAR
PAYID
PAYMETHOD
PM
PMLIST
PMLISTPMLISTTYPE
PMLISTTYPE
PMLISTTYPEPMLIST
PMTYPE
POPUP
POST
PSPID
PSWD
RECIPIENTACCOUNTNUMBER
RECIPIENTDOB
RECIPIENTLASTNAME
RECIPIENTZIP
REF
REFER
REFID
REFKIND
REF_CUSTOMERID
REF_CUSTOMERREF
REGISTRED
REMOTE_ADDR
REQGENFIELDS
RNPOFFERT
RTIMEOUT
RTIMEOUTREQUESTEDTIMEOUT
SCORINGCLIENT
SEQUENCETYPE
SETT_BATCH
SID
SIGNDATE
STATUS_3D
SUBSCRIPTION_ID
SUB_AM
SUB_AMOUNT
SUB_COM
SUB_COMMENT
SUB_CUR
SUB_ENDDATE
SUB_ORDERID

SUB_PERIOD_MOMENT
SUB_PERIOD_MOMENT_M
SUB_PERIOD_MOMENT_WW
SUB_PERIOD_NUMBER
SUB_PERIOD_NUMBER_D
SUB_PERIOD_NUMBER_M
SUB_PERIOD_NUMBER_WW
SUB_PERIOD_UNIT
SUB_STARTDATE
SUB_STATUS
TAAL
TAXINCLUDED*XX*
TBLBGCOLOR
TBLTXTCOLOR
TID
TITLE
TOTALAMOUNT
TP
TRACK2
TXTBADDR2
TXTCOLOR
TXTOKEN
TXTOKENTXTOKENPAYPAL
TXSHIPPING
TXSHIPPINGLOCATIONPROFILE
TXURL
TXVERIFIER
TYPE_COUNTRY
UCAF_AUTHENTICATION_DATA
UCAF_PAYMENT_CARD_CVC2
UCAF_PAYMENT_CARD_EXPDATE_MONTH
UCAF_PAYMENT_CARD_EXPDATE_YEAR
UCAF_PAYMENT_CARD_NUMBER
USERID
USERTYPE
VERSION
WBTU_MSISDN
WBTU_ORDERID
WEIGHTUNIT
WIN3DS
WITHROOT

16.2 SHA-OUT

AAVADDRESS
AAVCHECK
AAVMAIL
AAVNAME
AAVPHONE

AAVZIP
ACCEPTANCE
ALIAS
AMOUNT
BIC
BIN
BRAND
CARDNO
CCCTY
CN
COLLECTOR_BIC
COLLECTOR_IBAN
COMPLUS
CREATION_STATUS
CREDITDEBIT
CURRENCY
CVCCHECK
DCC_COMMPERCENTAGE
DCC_CONVAMOUNT
DCC_CONVCCY
DCC_EXCHRATE
DCC_EXCHRATESOURCE
DCC_EXCHRATETS
DCC_INDICATOR
DCC_MARGINPERCENTAGE
DCC_VALIDHOURS
DIGESTCARDNO
ECI
ED
EMAIL
ENCCARDNO
FXAMOUNT
FXCURRENCY
IP
IPCTY
MANDATEID
MOBILEMODE
NBREMAILUSAGE
NBRIPUSAGE
NBRIPUSAGE_ALLTX
NBRUSAGE
NCERROR
ORDERID
PAYID
PAYMENT_REFERENCE
PM
SCO_CATEGORY
SCORING

SEQUENCETYPE
SIGNDATE
STATUS
SUBBRAND
SUBSCRIPTION_ID
TRXDATE
VC