

Basic e-Commerce

Guide d'intégration technique pour le e-Commerce – Version 2.2



www.ogone.com
Copyright © Ogone 2010
Le contenu de ce document est protégé par le droit d'auteur.
Tous droits réservés.

Table des matières

Table des matières	2
1 Introduction	4
2 Environnement de test	5
2.1 Création d'un compte de test	5
2.2 Accéder à votre compte de test	5
2.3 Configurer votre compte de test	5
2.3.1 Configuration des méthodes de paiement	6
2.3.2 Configuration des informations techniques	6
2.4 Test de transactions et ses résultats	6
3 Procédure de vente	8
4 Lien entre le site internet du marchand et notre page de paiement	10
5 Sécurité : vérification avant le paiement	13
5.1 Referrer	13
5.2 Signature SHA-IN	13
5.2.1 Création de la chaîne	13
5.2.1 Module SHA-1	15
6 Apparence et impression de la page de paiement	16
7 Feedback au client sur la transaction	17
7.1 Sur l'écran	17
7.2 Par courrier électronique	17
7.3 Autres (Avancé)	17
8 Feedback au marchand sur la transaction	19
8.1 Back-office	19
8.2 Par courrier électronique	19

8.3	Requête sur votre page.....	19
8.4	Autres (Avancé)	21
9	Paramètres généraux de paiement	22
9.1	Code d'opération par défaut et procédure de télécollecte (paiement/data capture) par défaut	22
9.2	Traitement des transactions individuelles	23
10	Annexe 1: Paramètres à inclure dans le calcul SHA	24
10.1	SHA-IN	24
10.2	SHA-OUT.....	28

1 Introduction

Ce document explique la procédure de base d'intégration du module de e-Commerce.

Basic e-Commerce complète le **Guide d'utilisation Back-Office**. Veuillez vous référer au **Guide d'utilisation Back-Office** pour la configuration et la fonctionnalité du site d'administration.

Pour des informations d'intégration plus détaillées, veuillez vous référer au **Guide d'intégration Advanced e-Commerce**.

2 Environnement de test

Nous vous recommandons d'exécuter votre intégration dans notre environnement de test avant de migrer vers l'environnement de production. Notre environnement de test fonctionne de façon presque identique à l'environnement de production, sauf que nous n'envoyons pas la transaction à l'acquéreur et que nous ne vous facturons pas. Notre environnement de test vous permet de tester des paiements, changer la configuration de votre compte et ajuster l'intégration de notre système de paiement sur votre site Internet.

2.1 Création d'un compte de test

- Pour ouvrir un compte de test gratuit, visitez notre site Internet à l'adresse <http://www.ogone.com> .
- Cliquez sur le lien "Créez votre compte de test gratuit" en haut de la page.
- Complétez le formulaire (avec des informations correctes, puisque nous enverrons le mot de passe à l'adresse E-mail que vous allez indiquer !) et cliquez sur le bouton « Enregistrer ».
- Attendez de recevoir le courrier électronique de confirmation et celui contenant votre mot de passe (cela peut prendre un moment, car nous vérifions les renseignements que vous avez entrés).

2.2 Accéder à votre compte de test

Après avoir reçu le mot de passe par courrier électronique pour votre compte de test, vous pouvez accéder à votre compte comme suit :

- Visitez notre site Internet à l'adresse <http://www.ogone.com>.
- Cliquez sur le lien "Compte de test" sous 'Login Commerçant' en haut de la page.
- Entrez le PSPID que vous avez choisi lors de l'enregistrement de votre compte et le mot de passe (sensible à la casse !) que vous avez reçu par courrier électronique. Cliquez sur "Envoyer".

Lors de votre première ouverture de session avec le mot de passe que vous avez reçu par courrier électronique, le système vous demandera de modifier immédiatement le mot de passe et de choisir un nouveau mot de passe personnel.

2.3 Configurer votre compte de test

Lors de votre première ouverture de session dans votre compte, vous verrez une liste d'étapes à compléter sur la page d'accueil. Ces étapes concernent l'administration, méthodes de paiement et les détails techniques de votre compte de test. La configuration des renseignements administratifs est assez simple. La configuration des méthodes de paiement et des détails techniques est expliquée ci-dessous.

Vous pouvez commencer la configuration en cliquant le premier lien. À l'une des étapes, vous devez entrer vos renseignements de facturation. Dans l'environnement de test, vous ne recevrez pas de factures, mais on vous demandera d'entrer cette information de toutes façons. Vous pouvez choisir « Carte de crédit » comme méthode de facturation et entrer le numéro test de carte VISA 4111111111111111 avec une date d'expiration quelconque dans le future. Vous pouvez également choisir «not billed» comme méthode de facturation.

Lorsque toutes les étapes auront été complétées, vous pouvez demander l'activation de votre compte de test.

Une fois votre compte activé, si vous souhaitez changer certains détails, vous pouvez accéder aux différentes pages de configuration via votre menu. Cela est particulièrement utile pour la page « Information technique » puisque vous pouvez y changer certains détails pendant le test de votre intégration.

2.3.1 Configuration des méthodes de paiement

Pour sélectionner une méthode de paiement que vous voulez utiliser pour votre compte, cliquez simplement le bouton « Ajouter » adjacent à la méthode de paiement dans la liste des méthodes de paiement disponibles et remplissez la demande d'affiliation de carte. Vous pouvez compléter le formulaire avec des renseignements fictifs dans l'environnement de test. Cependant, dans l'environnement de production, vous devez remplir les renseignements d'affiliation exacts avec votre acquéreur, qui se trouvent sur le contrat signé avec celui-ci.

La méthode de paiement sera ajoutée à la liste « Méthodes de paiement sélectionnées ».

Vous pouvez accéder aux méthodes de paiement via le lien « Méthodes de paiement » de votre menu.

2.3.2 Configuration des informations techniques

Les chapitres suivants vous aideront à configurer la page Information Technique de votre compte. Au début de chaque chapitre, vous verrez une référence à la section correspondante dans la page Information Technique ou de votre site Internet, dépendant où vous devez agir.

Vous pouvez accéder aux paramètres techniques via le lien « Information Technique » de votre menu.

2.4 Test de transactions et ses résultats

Une fois votre compte entièrement configuré et actif, vous pouvez commencer à faire des tests de paiements. Vous pouvez le faire de votre site Internet ou d'une page test sur notre serveur, disponible dans l'onglet „Info de test“ de votre page „Information Technique“, qui représente la dernière page de votre panier d'achat. Vous pouvez utiliser cette page test si vous voulez commencer à faire des tests de paiement mais n'avez pas entièrement complété l'intégration dans votre site Internet.

Vous pouvez effectuer un test de paiement en suivant la procédure de vente décrite au Chapitre 3. Après avoir fait une transaction, vous pouvez voir les détails dans le back-office de votre compte. Lorsque vous êtes enregistré, cliquez sur le lien « Gestion Transactions » dans votre menu, entrez votre critère de sélection (la première fois, activez toutes les cases état et laissez les autres champs avec les valeurs par défaut) et voyez la liste des résultats. Consultez le **Guide d'utilisation Back-Office** pour plus d'information sur l'utilisation de back-office dans votre compte.

Ref	Merch ref	Orders (dd/mm/yyyy)	Status ?	Autor.	Payments (dd/mm/yyyy)	Total	Name	Method
1371176	order0021	12/09/2006 11:22:16	5- Authorized	testoff	0	75.10 EUR	Jack Smith	MasterCard
1371351	test1	12/09/2006 14:49:41	0-Invalid or incomplete		0	1.00 EUR	Bill Smith	CreditCard
1371518	Order7	12/09/2006 15:59:38	9-Payment requested	testoff	12/09/2006	345.00 EUR	Jack Russel	VISA

Les statuts de transaction les plus fréquents sont :

0 - Incomplète ou invalide

1 - Annulé par client

2 - Autorisation refusée

5 - Autorisé

9 - Paiement demandé

Pour plus d'information sur les différents états de transaction :

<https://secure.ogone.com/ncol/PAYMENTINFOS2.asp>

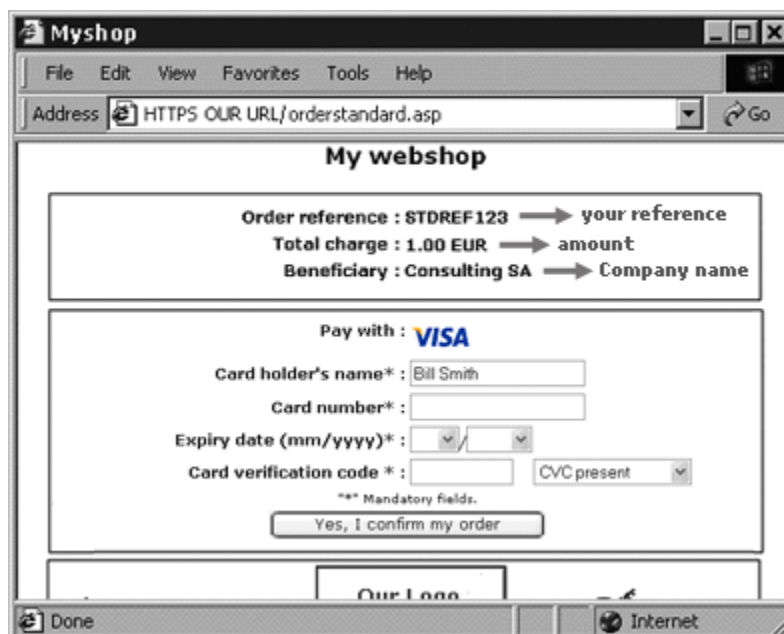
3 Procédure de vente

Les captures d'écran suivantes représentent la procédure de vente après l'intégration de base de votre site Internet avec notre système.



Sur votre site Internet, le client peut consulter un récapitulatif de sa commande. On lui demande de confirmer cette information avant de procéder à la page de paiement sécurisé.

Le bouton de confirmation est en fait la partie visible du « formulaire HTML » qui contient les champs cachés avec les données de paiement, ainsi que la redirection automatique du client en mode sécurisé vers la page paiement de notre serveur. Les champs cachés sont décrits au Chapitre 4 de ce document.



Sur notre page de paiement sécurisé, le client peut choisir n'importe laquelle des méthodes de paiement que vous avez sélectionnées.

Si c'est un paiement par carte de crédit, on demandera au client d'entrer son numéro de carte, etc. Le client peut confirmer ou annuler la demande de paiement.



Après avoir demandé le paiement de l'institution financière pertinente, nous présentons au client une page avec le résultat de son paiement.

Si le paiement a été refusé, une erreur est affichée et le client a la possibilité d'essayer à nouveau : il peut choisir une autre méthode de paiement ou changer les renseignements qu'il a introduits.

Une page spécifique sur votre site Internet peut aussi être affichée au client, dépendant du résultat de la transaction. Pour plus d'information, veuillez vous référer au Chapitre 7 de ce document.

4 Lien entre le site internet du marchand et notre page de paiement

Où configurer? Votre site Internet (panier d'achat)

Le lien entre votre site Internet et notre page de paiement de e-Commerce doit être établi sur la dernière page du panier d'achat sur votre site Internet : c'est-à-dire la dernière page de votre site présentée à l'acheteur.

Un formulaire avec des champs html cachés contenant les données de la commande doit être intégré dans la dernière page. Le bloc de code que vous devrez coller dans la dernière page de votre panier d'achat est le suivant :

```
<form method="post" action="https://secure.ogone.com/ncol/XXXX/orderstandard.asp" id=form1
name=form1>
```

```
<!-- paramètres 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="">
<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="">
<!-- vérification avant le paiement : chapitre 5 -->
<input type="hidden" name="SHASign" value="">
<!-- apparence et impression : chapitre 6 -->
<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="">
```

```

<!-- redirection après la transaction : chapitre 7 -->
<input type="hidden" name="accepturl" value="">
<input type="hidden" name="declineurl" value="">
<input type="hidden" name="exceptionurl" value="">
<input type="hidden" name="cancelurl" value="">
<input type="submit" value="" id=submit2 name=submit2>
</form>

```

Bien que les paramètres obligatoires soient le PSPID, orderID, amount, currency et language, nous recommandons fortement néanmoins de nous envoyer le nom du client, l'adresse électronique du client, l'adresse, la ville, le code postal, le pays, et le numéro de téléphone puisque ce sont des outils utiles pour combattre les fraudes.

Un sommaire des champs cachés utilisés pour transmettre les « paramètres généraux » à notre système (les autres champs sont décrits dans les chapitres suivants) est donné ci-bas :

Champ	Usage
PSPID	Votre nom d'affiliation dans notre système
orderID	Votre numéro de commande (référence du marchand). Le système vérifie que le paiement n'a pas été demandé deux fois pour la même commande. L'orderId doit être assigné dynamiquement.
amount	Montant à payer MULTIPLIÉ PAR 100 puisque le format du montant ne doit pas contenir de décimales ou autres séparateurs. Le montant doit être assigné dynamiquement.
currency	Devise pour la commande en code ISO alpha. Par exemple : EUR, USD, GBP, ...
language	Langue du client. Par exemple : en_US, nl_NL, fr_FR, ...
CN	Le nom du client. Sera pré-initialisé (mais toujours éditable) dans le champ Nom du Client des renseignements de la carte de crédit.
EMAIL	L'adresse électronique du client
owneraddress	L'adresse du client
ownerZIP	Le code postal du client
ownertown	Nom de la ville du client
ownercty	Le pays du client
ownertelno	Le numéro de téléphone du client

Pour de plus amples détails techniques au sujet de ces champs, veuillez vous référer au *Parameter Cookbook en ligne*.

L'action du formulaire sera la page de traitement de notre système de e-Commerce.

Dans l'environnement de TEST, l'URL pour l'action sera :
<https://secure.ogone.com/ncol/test/orderstandard.asp>.

Dans l'environnement de PRODUCTION, l'URL pour l'action sera :
<https://secure.ogone.com/ncol/prod/orderstandard.asp>

IMPORTANT : Lorsque vous passez au compte de PRODUCTION, vous devez impérativement remplacer le « test » par « prod ». Un oubli aura pour conséquence d'envoyer vos transactions en environnement de test où elles ne seront pas envoyées aux acquéreurs et aux banques.

5 Sécurité : vérification avant le paiement

Où configurer? Information Technique – onglet „Contrôle des données et d'origine” – section „Contrôles pour e-Commerce”

5.1 Referrer

Notre système vérifie l'origine de la demande de paiement, c'est-à-dire l'URL (page Web) de l'origine de la commande. Cet URL est appelé le « referrer ».

Vous devez remplir l'URL de votre page Web contenant le formulaire de commande avec les champs cachés dans la section „Contrôles pour e-Commerce” de l'onglet „Contrôle des données et d'origine” de la page Information Technique dans votre compte (Champ URL).

Vous pouvez entrer différents URLs, séparés par `;'. Le(s) URL(s) doivent toujours commencer par http:// ou https://.

Si vous entrez une mauvaise URL, vous verrez l'erreur « *unknown order/1/r* » sur la page de paiement.

5.2 Signature SHA-IN

Étant donné que la vérification du *referrer* n'est pas exempte d'erreur, notre système peut effectuer une vérification de données avant de traiter le paiement afin de s'assurer de l'exactitude et de l'intégrité des données de la commande. Cette vérification de données n'est pas obligatoire, mais fortement recommandée. Si vous ne l'utilisez pas, notre système ne vous autorisera pas à configurer „Vente” comme code d'opération par défaut, ni Télécollecte automatique par défaut (voir chapitre 9) ; vous devrez utiliser une procédure en 2 phases – autorisation suivie d'une capture de données manuelle – pour traiter les transactions par carte de crédit.

Nous proposons SHA-1, SHA-256 et SHA-512 comme méthodes de vérification des données. Pour chaque commande, votre serveur génère une chaîne de caractères unique (appelée un condensé), hachée avec l'algorithme SHA de votre choix.

IMPORTANT : Si vous ne pouvez pas l'intégrer, mais ne souhaitez pas utiliser une procédure manuelle en deux étapes pour vos paiements par carte de crédit, vous pouvez nous adresser une demande signée par fax dans laquelle vous nous demanderez de désactiver pour vous cette vérification de données. Toutefois, dans pareil cas, vous serez responsable de l'exactitude des données de la commande et de leur intégrité dans le processus de redirection.

5.2.1 Création de la chaîne

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 1. Veuillez observer que ces valeurs sont sensibles à la casse lors de leur compilation pour former la chaîne avant le hachage !

Important : tous les noms de paramètre devraient être en MAJUSCULE (pour éviter les problèmes de casse)

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://secure.ogone.com/ncol/test/testsha.asp>

Exemple d'un calcul SHA-1-IN élémentaire

paramètres (dans l'ordre alphabétique)

amount : 15.00 -> 1500

currency : EUR

Operation : RES

orderID: 1234

PSPID : MyPSPID

Clé SHA

Mysecretsig1875!?

chaîne à hacher

AMOUNT=1500Mysecretsig1875!?CURRENCY=EURMysecretsig1875!?OPERATION=RESMysecretsig1875!?
ORDERID=1234Mysecretsig1875!?PSPID=MyPSPIDMysecretsig1875!?

condensé obtenu (SHA-1)

EB52902BCC4B50DC1250E5A7C1068ECF97751256

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».

Ce qui suit est le champ caché utilisé pour transmettre la signature SHA à notre système :

Champ	Usage
SHASign	Caractère de chaîne unique pour la validation des données de la commande. Une chaîne hachée avec l'algorithme SHA-1 sera toujours 40 caractères en longueur.

5.2.1 Module SHA-1

Pour hacher une chaîne et nous l'envoyer, en général, vous devez installer un module SHA-1 sur votre serveur. Si vous travaillez dans un environnement Windows 2000/asp, nous pouvons vous fournir un dll qui inclut une méthode pour hacher la chaîne en utilisant un SHA-1. Vous pouvez télécharger la dll via le lien support > documentation dans votre compte.

Du fait qu'il a plusieurs combinaisons de systèmes d'exploitation (numéros de version/patches) et langages de programmation, nous ne sommes pas responsables de toute erreur sur votre serveur à l'installation et/ou au traitement.

Les modules SHA-1 étant en libre téléchargement sur Internet, vous avez toute latitude pour trouver le module le plus adapté à votre serveur. Afin de vous assister dans votre recherche, nous avons compilé une liste des sites suivants :

Information générale sur SHA à W3.org :

http://www.w3.org/PICS/DSig/SHA1_1_0.html

.NET/SHA1 :

<http://msdn2.microsoft.com/en-us/library/system.security.cryptography.sha1managed.aspx>

PHP/SHA1 :

<http://www.php.net/manual/en/ref.mhash.php>

6 Apparence et impression de la page de paiement

Où configurer? Votre site Internet (panier d'achat)

Lorsque notre système de e-Commerce demande au client les détails de sa carte de crédit, le client est sur notre serveur sécurisé. Pour maintenir l'apparence de votre site Internet pendant la procédure de paiement, vous pouvez personnaliser nos templates statiques.

La page de template statique est une page d'apparence générique de notre côté, mais vous pouvez changer l'apparence de certains éléments de la page de paiement ou ajouter votre logo simplement en ajoutant des champs cachés dans le formulaire que vous nous envoyez (cf. Chapitre 4) :

Voici les champs cachés utilisés pour transmettre les paramètres d'apparence et d'impression de notre système :

Champ	Usage	Valeur Défaut
TITLE	Titre et en-tête de la page	—
BGCOLOR	Couleur de fond	white
TXTCOLOR	Couleur du texte	black
TBLBGCOLOR	Couleur de fond des tableaux	white
TBLTXTCOLOR	Couleur du texte des tableaux	black
BUTTONBGCOLOR	Bouton pour couleur de fond	—
BUTTONTXTCOLOR	Bouton pour couleur du texte	black
FONTTYPE	Famille de fontes	Verdana
LOGO	<p>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.</p> <p>Si vous ne possédez pas un environnement sécurisé pour enregistrer votre image, vous pouvez envoyer un fichier JPG ou GIF (et votre PSPID) à support@ogone.com (seulement pour les comptes de production puisque c'est une option payante ! Activez l'option « Logo Hosting » avant de nous envoyer votre logo). Si le logo est enregistré sur nos serveurs, vous n'aurez besoin que d'entrer le nom du fichier, et non l'URL au complet.</p>	—

Pour de plus amples détails techniques au sujet de ces champs, veuillez vous référer au *Parameter Cookbook* en ligne.

Les couleurs peuvent être spécifiées par leur code hexadécimal (#FFFFFF) ou leur nom (white). Veuillez vérifier en premier comment les couleurs apparaîtront sur les différents navigateurs.

Il est également possible d'utiliser un template spécifique ou dynamique. Cependant, ceci exige une intégration avancée. Vous trouverez plus amples informations dans le **Guide d'intégration Advanced e-Commerce**.

7 Feedback au client sur la transaction

Où configurer? Votre site Internet (panier d'achat), Information technique – l'onglet "E-mails de transaction" – section " E-mails pour le client"

7.1 Sur l'écran

Si vous ne précisez rien, notre système affiche un message standard au client : « Votre paiement a été autorisé » ou « La transaction a été refusée ». Ce message est inséré dans la page template (paiement), qui contient aussi un lien pour votre page d'accueil.

Cependant, vous pouvez également rediriger votre client vers une page HTML sur votre site Internet dépendant du résultat de paiement. Dans les champs cachés de votre formulaire de commande, vous pouvez envoyer 4 URLs (accepturl, exceptionurl, cancelurl et declineurl) où notre système va rediriger le client à la fin du processus de paiement :

Voici les champs cachés utilisés pour transmettre les URL's :

Champ	Usage
accepturl	URL de la page Web pour afficher au client que le paiement a été autorisé (statut 5), accepté (statut 9) ou en attente d'être accepté (statut 51 ou 91).
declineurl	URL de la page Web pour afficher au client que l'acquéreur a refusé l'autorisation (statut 2) plus du maximum du nombre d'essais autorisés.
exceptionurl	URL de la page Web pour afficher au client que le résultat du paiement est incertain (statut 52 ou 92). Si ce champ est vide, l'accepturl sera affiché au client à la place.
cancelurl	URL de la page Web pour afficher au client qu'il a annulé le paiement (statut 1). Si ce champ est vide, le declineurl sera affiché au client à la place.

Pour de plus amples détails techniques au sujet de ces champs, veuillez vous référer au Parameter Cookbook en ligne.

Vous pouvez également configurer ces URL's dans la section „Redirection HTTP dans le navigateur” de l'onglet „Retour des informations de transaction”.

7.2 Par courrier électronique

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.

7.3 Autres (Avancé)

Il est également possible d'afficher au client, entre autres, une réponse hautement personnalisée dans le navigateur ou simplement avec un texte supplémentaire. Cependant, ceci demande une intégration

avancée. Vous trouverez plus amples informations dans le **Guide d'intégration Advanced e-Commerce**.

8 Feedback au marchand sur la transaction

Où configurer? Votre site Internet (base de données), Information technique – l’onglet "E-mails de transaction" – section " E-mails pour le marchand", Information technique – l’onglet " Retour des informations de transaction" – section " Redirection HTTP dans le navigateur"

8.1 Back-office

Vous pouvez consulter les résultats des transactions dans le back-office de votre compte. Lorsque vous êtes enregistrés, cliquez sur le lien « Historique Financier » ou le lien « Gestion Transactions » dans votre menu, entrez vos critères de sélection et consultez la liste des résultats. Veuillez vous référer au **Guide d'utilisation Back-Office** pour plus d'informations au sujet de l'utilisation de back-office dans votre compte.

8.2 Par courrier électronique

Vous pouvez recevoir un courrier électronique de confirmation de paiement de notre système pour chaque transaction (option de configuration dans la section „E-mails pour le marchand“ de l’onglet „E-mails de transaction“ de la page Information Technique).

8.3 Requête sur votre page

Lorsqu'un paiement est effectué, nous pouvons envoyer la liste de paramètres suivant dans une requête sur votre accept-, exception-, cancel- ou declineurl (cf. Chapitre 7.1) pour vous permettre de mettre à jour votre base de données :

Paramètre	Valeur
orderId	Votre référence pour la commande
amount	Montant de la commande (non multiplié par 100)
currency	Devise de la commande
PM	Méthode de paiement
ACCEPTANCE	Code d'acceptation donné par l'acquéreur
STATUS	Statut de la transaction
CARDNO	Numéro de carte (masqué)
PAYID	Référence de paiement dans notre système
NC ERROR	Code d'erreur
BRAND	Type de carte (notre système le détermine à partir du numéro de la carte) ou information similaire pour les autres méthodes de paiement.
SHASIGN	Signature SHA composée par notre système, si SHA-1-OUT configurée par vous.

Vous pouvez activer cette option dans la section „Redirection HTTP dans le navigateur” de l’onglet „Retour des informations de transaction” de la page Information Technique („Je veux recevoir les paramètres de transaction en retour dans les URL lors de la redirection”).

IMPORTANT: Vous devez utiliser une signature SHA-out pour vérifier le contenu de la demande lorsque vous utilisez cette option pour empêcher que les clients falsifient les renseignements dans le champ URL et causent une mise à jour incorrecte de la base de données.

Si vous ne configurez pas de signature SHA-out dans votre compte, la liste de paramètres ne sera pas transmise dans nos requêtes sur vos URL.

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 marchand, sous l’onglet “Retour d’Information sur la transaction”, section “Tous les modes de soumission des transactions.” Pour obtenir la liste complète des paramètres à inclure dans le condensé SHA, veuillez vous reporter à l’Annexe 1. Veuillez noter que ces valeurs sont toutes sensibles à la casse.

Important : tous les noms de paramètre devraient être en MAJUSCULE (pour éviter les problèmes de casse)

Tout comme nous récréons le condensé pour valider l’input de la transaction avec le SHA-IN, vous devez reconstruire le hachage, en utilisant cette fois la phrase passe SHA-OUT et les paramètres obtenus de notre système.

Si le résultat n’est pas identique, il se pourrait que les paramètres de la demande aient été modifiés. Cette vérification permet de d’assurer de l’exactitude et de l’intégrité des valeurs de paramètre envoyées dans la requête.

Exemple d'un calcul SHA-1-OUT élémentaire

ACCEPTATION : 1234
amount : 15
BRAND : VISA
CARDNO : xxxxxxxxxxxx1111
currency : EUR
NCERROR: 0
orderID: 12
PAYID: 32100123
PM : CreditCard
STATUS : 9

Clé SHA

Mysecretsig1875!?

Chaîne entière à hacher :

ACCEPTANCE=1234Mysecretsig1875!?!AMOUNT=1500Mysecretsig1875!?!BRAND=VISAMysecretsig1875!?!CARDNO=xxxxxxxxxxxx1111Mysecretsig1875!?!CURRENCY=EURMysecretsig1875!?!NCERROR=0Mysecretsig1875!?!ORDERID=12Mysecretsig1875!?!PAYID=32100123Mysecretsig1875!?!PM=CreditCardMysecretsig1875!?!STATUS=9Mysecretsig1875!?!?

Condensé obtenu (SHA-1) :

28B64901DF2528AD100609163BDF73E3EF92F3D4

Veuillez vous référer au Chapitre 5 pour plus d’informations générales sur le module SHA-1.

8.4 Autres (Avancé)

Il est également possible de recevoir une requête avec paramètres de transaction de notre part sur une page spécifique de votre côté qui n'est pas visible par le client. Cependant, ceci demande une intégration avancée. Vous trouverez plus d'information sur ce sujet et autres options dans le **Guide d'intégration Advanced e-Commerce**.

9 Paramètres généraux de paiement

IMPORTANT: ce chapitre est applicable seulement pour les méthodes de paiements telles que les cartes de crédit qui permettent de réserver l'argent du client sans le facturer immédiatement.

La possibilité de travailler en deux phases (autorisation + télécollecte) et la possibilité de travailler en ligne ou hors-ligne dépend des méthodes de paiement que vous souhaitez appliquer. (Voir le module en ligne **Payment Methods Processing/Procedure overview**).

Où configurer? Information technique – Paramètres de transaction globaux

9.1 Code d'opération par défaut et procédure de télécollecte (paiement/data capture) par défaut

Pour certaines méthodes de paiement (principalement les cartes de crédit), les transactions sont exécutées en deux phases: l'autorisation et la télécollecte (data capture, demande de paiement). Durant la phase d'autorisation, le montant de la transaction est soit réservé sur la carte du client ou soit on vérifie s'il y a correspondance avec une liste noire. Dans la phase de télécollecte (demande de paiement), votre acquéreur est invité à prendre la réserve ou la correspondance sur la liste noire de la carte ou du compte du client et de la transférer à votre compte de banque.

Sur base de ces deux étapes, vous avez le choix entre deux codes d'opération par défaut:

- **Autorisation:** notre système ne demande qu'une autorisation pour exécuter les étapes de l'autorisation et de la télécollecte (demande de paiement) séparément à des moments différents (l'argent reste sur le compte du client jusqu'à l'exécution d'une télécollecte (demande de paiement)).
- **Vente:** notre système demande automatiquement le paiement (transfert du montant) juste après une autorisation réussie. Cette procédure est souvent employée pour les marchandises / biens livrés en ligne.

Si vous avez "Autorisation" comme code d'opération par défaut pour votre compte ou que vous avez inclus le code d'opération "Autorisation" dans les détails de la transaction, une télécollecte devra être exécutée sur la transaction pour demander le paiement.

Trois procédures de télécollecte (demande de paiement, data capture) sont possibles:

- **Télécollecte (data capture) par le marchand (manuelle ou automatique):** pour demander le transfert du montant réservé sur votre compte bancaire, vous devez entrer dans le module de gestion (back-office) et demander la télécollecte (paiement) pour la transaction spécifique.

Vous pouvez aussi automatiser le traitement des données en nous transmettant les demandes de paiement par lot ou via une requête de serveur à serveur.

Cette procédure est souvent appliquée si le marchand doit vérifier ses stocks avant d'expédier les marchandises commandées.

- **Télécollecte (data capture) automatique par notre système à la fin de la journée:** notre système demande automatiquement le paiement (télécollecte) à partir de minuit, heure GMT+1.

- **Télécollecte (data capture) automatique par notre système après x jours:** notre système demande automatiquement le paiement (télécollecte) après x jours (si vous n'avez pas annulé l'autorisation).

Le nombre de jours minimum que vous pouvez saisir est "2" puisque "1" entraînerait automatiquement la requête du paiement à partir de minuit, soit comme dans la procédure "Télécollecte automatique par notre système à la fin de la journée".

Cette procédure est souvent employée pour les marchandises / services livrés dans un délai spécifique.

9.2 Traitement des transactions individuelles

Des transactions individuelles peuvent être traitées de trois façons:

- **"Toujours online (en ligne, immédiat)":** la requête de transaction est transmise immédiatement à l'acquéreur pendant que le client est connecté (solution idéale pour les marchandises / services livrés en ligne).
- **"Online mais basculer en offline durant les périodes d'indisponibilité du système acquéreur":** si vous souhaitez effectuer un traitement en ligne mais que vous ne voulez pas rater des transactions si le système de compensation en ligne de l'acquéreur est temporairement indisponible, vous pouvez autoriser un traitement hors ligne dans ces conditions spécifiques.

Nous stockerons les transactions en provenance de votre site Web pendant l'indisponibilité de votre acquéreur et les traiterons hors ligne dès que le système de compensation de l'acquéreur sera rétabli. (Ne convient pas pour des services qui sont activés en ligne juste après la transaction!)

- **"Toujours offline (hors-ligne, différé)":** nous enregistrons la transaction et la traitons ultérieurement (max. 4 heures). Cette méthode est légèrement plus rapide pour le client, car nous n'envoyons pas la requête à l'acquéreur immédiatement (peut être employée pour des marchandises / services qui ne doivent pas être livrés en ligne). Néanmoins, le client ne verra pas immédiatement le résultat de la transaction / commande. Le traitement hors-ligne n'est pas possible pour toutes les méthodes de paiement.

10 Annexe 1: Paramètres à inclure dans le calcul SHA

10.1 SHA-IN

ACCEPTURL
ADDMATCH
ADDRMATCH
AIAIRNAME
AIAIRTAX
AIBOOKIND*XX*
AICARRIER*XX*
AICHDET
AICLASS*XX*
AICONJTI
AIDESTCITY*XX*
AIDESTCITYL*XX*
AIEXPASNAME*XX*
AIEYCD
AIFLDATE*XX*
AIFLNUM*XX*
AIIRST
AIORCITY*XX*
AIORCITYL*XX*
AIPASNAME
AISTOPOV*XX*
AITIDATE
AITINUM
AITYPCH
AIVATAMNT
AIVATAPPL
ALIAS
ALIASOPERATION
ALIASUSAGE
ALLOWCORRECTION
AMOUNT
AMOUNT*XX*
AMOUNTHTVA
AMOUNTTVA
BACKURL
BGCOLOR
BRAND
BRANDVISUAL
BUTTONBGCOLOR
BUTTONTXTCOLOR
CANCELURL
CARDNO
CATALOGURL
CAVV_3D
CAVVALGORITHM_3D
CERTID
CHECK_AAV
CIVILITY
CN
COM
COMPLUS
COSTCENTER
COSTCODE
CREDITCODE
CUID

CURRENCY
CVC
DATA
DATATYPE
DATEIN
DATEOUT
DECLINEURL
DISCOUNTRATE
ECI
ECOM_BILLTO_POSTAL_CITY
ECOM_BILLTO_POSTAL_COUNTRYCODE
ECOM_BILLTO_POSTAL_NAME_FIRST
ECOM_BILLTO_POSTAL_NAME_LAST
ECOM_BILLTO_POSTAL_POSTALCODE
ECOM_BILLTO_POSTAL_STREET_LINE1
ECOM_BILLTO_POSTAL_STREET_LINE2
ECOM_BILLTO_POSTAL_STREET_NUMBER
ECOM_CONSUMERID
ECOM_CONSUMERORDERID
ECOM_CONSUMERUSERALIAS
ECOM_PAYMENT_CARD_EXPDATE_MONTH
ECOM_PAYMENT_CARD_EXPDATE_YEAR
ECOM_PAYMENT_CARD_NAME
ECOM_PAYMENT_CARD_VERIFICATION
ECOM_SHIPTO_COMPANY
ECOM_SHIPTO_DOB
ECOM_SHIPTO_ONLINE_EMAIL
ECOM_SHIPTO_POSTAL_CITY
ECOM_SHIPTO_POSTAL_COUNTRYCODE
ECOM_SHIPTO_POSTAL_NAME_FIRST
ECOM_SHIPTO_POSTAL_NAME_LAST
ECOM_SHIPTO_POSTAL_POSTALCODE
ECOM_SHIPTO_POSTAL_STREET_LINE1
ECOM_SHIPTO_POSTAL_STREET_LINE2
ECOM_SHIPTO_POSTAL_STREET_NUMBER
ECOM_SHIPTO_TELECOM_FAX_NUMBER
ECOM_SHIPTO_TELECOM_PHONE_NUMBER
ECOM_SHIPTO_TVA
ED
EMAIL
EXCEPTIONURL
EXCLPMLIST
EXECUTIONDATE*XX*
FIRSTCALL
FLAG3D
FONTTYPE
FORCECODE1
FORCECODE2
FORCECODEHASH
FORCEPROCESS
FORCETP
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
INVDATA

INVDISCOUNT
INVLEVEL
INVORDERID
ISSUERID
ITEMCATEGORY*XX*
ITEMDISCOUNT*XX*
ITEMID*XX*
ITEMNAME*XX*
ITEMPRICE*XX*
ITEMQUANT*XX*
ITEMUNITOFMEASURE*XX*
ITEMVATCODE*XX*
LANGUAGE
LEVEL1AUTHCPC
LIDEXCL*XX*
LIMITCLIENTSCRIPTUSAGE
LINE_REF
LIST_BIN
LIST_COUNTRIES
LOGO
MERCHANTID
MODE
MTIME
MVER
NETAMOUNT
OPERATION
ORDERID
ORIG
OR_INVORDERID
OR_ORDERID
OWNERADDRESS
OWNERADDRESS2
OWNERCTY
OWNERTELNO
OWNERTOWN
OWNERZIP
PAIDAMOUNT
PARAMPLUS
PARAMVAR
PAYID
PAYMETHOD
PM
PMLIST
PMLISTPMLISTTYPE
PMLISTTYPE
PMLISTTYPEPMLIST
PMTYPE
POPUP
POST
PSPID
PSWD
REF
REFER
REFID
REFKIND
REF_CUSTOMERID
REF_CUSTOMERREF
REMOTE_ADDR
REQGENFIELDS
RTIMEOUT
RTIMEOUTREQUESTEDTIMEOUT
SCORINGCLIENT
SETT_BATCH
SID
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
TXTOKENXTOKENPAYPAL
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

10.2 SHA-OUT

AAVADDRESS
AAVCHECK
AAVZIP
ACCEPTANCE
ALIAS
AMOUNT
BRAND
CARDNO
CCCTY
CN
COMPLUS
CREATION_STATUS
CURRENCY
CVCCHECK
DCC_COMMPERCENTAGE
DCC_CONVAMOUNT
DCC_CONVCCY
DCC_EXCHRATE
DCC_EXCHRATESOURCE
DCC_EXCHRATETS
DCC_INDICATOR
DCC_MARGINPERCENTAGE
DCC_VALIDHOURS
DIGESTCARDNO
ECI
ED
ENCCARDNO
IP
IPCTY
NBREMAILUSAGE
NBRIPIUSAGE
NBRIPIUSAGE_ALLTX
NBRUSAGE
NCERROR
ORDERID
PAYID
PM
SCO_CATEGORY
SCORING
STATUS
SUBSCRIPTION_ID
TRXDATE
VC