

## Intégration avec Ogone e-Commerce



## Table des matières

### 1. Introduction

### 2. Page Information technique

### 3. Processus de vente

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

#### 4.1 Où configurer?

#### 4.2 Paramètres de formulaire

#### 4.3 L'action du formulaire

### 5. Sécurité : vérification avant le paiement

#### 5.1 Signature SHA-IN

##### 5.1.1 Création de la chaîne

#### 5.2 Referrer (Référerant)

### 6. Aspect de la page de paiement

#### 6.1 Présentation de la page de paiement (modèle statique)

##### 6.1.1 Hébergement de logo

#### 6.2 Modèle hébergé par Ogone (modèle statique)

##### 6.2.1 Champs cachés

##### 6.2.2 Zone de paiement (Payment zone)

##### 6.2.3 Feuille de style

#### 6.3 Mise en page basée sur le modèle (modèle dynamique)

##### 6.3.1 Champs masqués

##### 6.3.2 Zone de paiement (Payment zone)

##### 6.3.3 Comportement dynamique

#### 6.3.4 Feuille de style

#### 6.3.5 Performance

### 6.4 Modèle pour mobile

#### 6.4.1 Paramètres de présentation

#### 6.4.2 Modèle

#### 6.4.3 Feuilles de style (CSS)

#### 6.4.4 Exemples de pages

### 6.5 Gestionnaire de fichiers modèles

#### 6.5.1 Télécharger des fichiers modèles

#### 6.5.2 Contrôler et gérer les fichiers téléchargés

#### 6.5.3 Intégration

### 6.6 Contrôle de la sécurité des modèles

### 6.7 Cadenas de l'environnement sécurisé

### 6.8 Page de paiement dans un iframe

## 7. Retour d'information sur la transaction

### 7.1 Réaction par défaut

### 7.2 Redirection en fonction du résultat du paiement

### 7.3 Option mise à jour de la base de données

#### 7.3.1 SHA-OUT

### 7.4 Requête de réponse directes (après paiement)

#### 7.4.1 URL d'après-paiement

#### 7.4.2 Plannification de la requête d'informations

#### 7.4.3 Réponse envoyée au client

#### 7.4.4 Requête http pour les changements de statut

### 7.5 Paramètres du retour d'information

#### 7.5.1 Paramètres du retour d'information dynamiques

#### 7.5.2 Paramètres du retour d'information

## 7.6 Réinitialisation du retour d'information

## 7.7 E-mails de confirmation

### 7.7.1 E-mails envoyés au marchand

### 7.7.2 E-mails envoyés au client

## 8. e-Commerce via e-mail

## 9. Moyen de paiement et caractéristiques de la page de paiement

### 9.1 Choix du moyen de paiement du côté du marchand

#### 9.1.1 Afficher un moyen de paiement déterminé

#### 9.1.2 Permettre au client de choisir un autre moyen de paiement : BACKURL

### 9.2 Afficher une liste déterminée de moyens de paiement

### 9.3 Exclure une liste déterminée de moyens de paiement

### 9.4 Présentation des moyens de paiement

### 9.5 Fenêtre pour 3-D Secure

### 9.6 Subdivision en cartes de crédit/débit

## 10. Autres champs masqués facultatifs

### 10.1 Code Opération

### 10.2 Champ Utilisateur

## 1. Introduction

La documentation e-Commerce détaille l'intégration d'e-Commerce sur votre site Web.

## 2. Page Information technique

Dans votre compte Ogone, vous trouverez la page d'Information technique via "Configuration" dans le menu supérieur.

A la page d'information technique, vous trouverez le "i" icône pour expliquer le contexte particulier.

### 3. Processus de vente

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

YOUR WEBSITE

**My Webshop**

Item	Price	Quantity	Total
Book	23 EUR	1	23 EUR
CD	11 EUR	2	22 EUR
Delivery costs			4 EUR
<b>Total</b>			<b>49 EUR</b>

<FORM... /FORM>

Online Secure Payment

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 [Lien entre le site internet du marchand et notre page de paiement](#) de ce document.

HTTPS://YOUR URL/orderstandard.asp

**My webshop**

Order reference : ORDER123

Total charge : 49.00 EUR

Beneficiary : Webshop

your reference

amount

your company name

Pay with : **VISA**

Card holder's name\* : Bill Smith

Card number\* :

Expiry date (mm/yyyy)\* : 05 / 2016

Card verification code\* :  CVC present

\* Mandatory Fields

THE LOGO OF YOUR ACQUIRER

Our Logo


[About](#) | [Privacy policy](#) | [Security](#) | [Legal info](#)

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.

HTTPS://OUR.URL/order\_Agree.asp

**My webshop**  
Order reference : ORDER123  
Total charge : 49.00 EUR  
Beneficiary : Webshop  
**Authorised**  
Payment reference : 15987181

 THE LOGO OF  
YOUR ACQUIRER

Our Logo



[About](#) | [Privacy policy](#) | [Security](#) | [Legal info](#)

[Back to merchant site](#)

Après avoir demandé le paiement à 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 introduit.

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 [Feedback au client sur la transaction](#) de ce document.



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

### 4.1 Où configurer?

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/test/orderstandard.asp / orderstandard_utf8.asp" id=form1 name=form1>

<!-- paramètres généraux : voir Paramètres de formulaire -->
<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 : voir Sécurité : vérification avant le paiement -->
<input type="hidden" name="SHASIGN" value="">

<!-- apparence et impression: voir Apparence 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="">

<!-- redirection après la transaction : voir Feedback au client sur la transaction -->
<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>
```

### 4.2 Paramètres de formulaire

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 [lutter contre les fraudes](#).

Vous trouverez ci-dessous un aperçu des champs cachés utilisés pour transmettre les « paramètres généraux » à notre système (les autres champs sont décrits dans les chapitres suivants) :

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, ...  Le nom du client.
CN	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

### 4.3 L'action du formulaire

```
<form method="post" action="https://secure.ogone.com/ncol/test/orderstandard.asp / orderstandard_utf8.asp" id=form1 name=form1>
```

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 / orderstandard\\_utf8.asp](https://secure.ogone.com/ncol/test/orderstandard.asp / orderstandard_utf8.asp)
- Dans l'environnement de PRODUCTION, l'URL pour l'action sera : <https://secure.ogone.com/ncol/prod/orderstandard.asp />

orderstandard\_utf8.asp

**Changez "test" à "prod"**

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

### 5.1 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.

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.

#### 5.1.1 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 PARAMETRE=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" .

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

#### Important

- Tous les paramètres que vous envoyez (et qui apparaissent dans la liste [SHA-IN params](#)), seront inclus dans la chaîne.
- Tous les noms de paramètres doivent être en MAJUSCULES (pour éviter toute confusion)
- Tous les paramètres doivent être classés dans l'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 [ici](#).

#### Exemple d'un calcul SHA-1-IN élémentaire

Paramètres (dans l'ordre alphabétique) :

AMOUNT=1500 (15.00 x100)  
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 (SHA-1) :

F4CC376CD7A834D997B91598FA747825A238BE0A

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	Chaîne de caractères unique pour la validation des données de la commande.

## 5.2 Referrer (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 ».

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.

### Important

- 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.

Although the referrer allows our system to identify the origin of an order, it does not guarantee the integrity of the data. Therefore, our system requires the use of an SHA signature.

Des erreurs liées au référant sont possibles, par ex., « unknown order/1/r » et « unknown order/0/r ». Veuillez vous reporter à [Erreurs possibles](#) pour de plus amples informations sur ces erreurs.



## 6. Aspect de la page de paiement

On distingue deux types d'informations sur la page de paiement hébergée :

- Informations statiques (par ex. votre logo)
- Informations de paiement (par ex. référence de la commande, champs dans lesquels le client saisit les informations de sa carte, etc.).

Les informations statiques proviennent de la présentation commune de notre système ou d'une page de modèle d'un commerçant spécifique. Notre système ajoute les informations de paiement de manière dynamique pour chaque transaction. Le commerçant a toutefois la possibilité d'adapter l'aspect de ces informations de paiement au moyen de styles HTML.

Pour conserver réellement l'aspect de votre site web pendant le processus de paiement, vous pouvez personnaliser la conception de la page de paiement en appliquant un modèle statique ou une page de modèle dynamique :

- Dans le cas d'un modèle statique, vos fichiers de modèles sont hébergés en toute sécurité sur notre environnement certifié PCI-DSS. Vous pouvez facilement gérer vos fichiers de modèles en utilisant le gestionnaire de fichiers de modèles dans votre compte Ogone.
- Si vous souhaitez héberger votre modèle de votre côté, pour vous accorder plus de flexibilité et un comportement "dynamique", vous devez utiliser un modèle dynamique.

### 6.1 Présentation de la page de paiement (modèle statique)

Vous pouvez modifier l'aspect de certains éléments de la page de paiement et ajouter votre logo, simplement en insérant quelques champs cachés dans le formulaire que vous nous envoyez.

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	white
TXTCOLOR	Couleur du texte	black
TBLBGCOLOR	Couleur de fond du tableau	white
TBLTXTCOLOR	Couleur du texte du tableau	black
BUTTONBGCOLOR	Couleur de fond du bouton	-

Champ	Objet	Valeur par défaut
BUTTONTXTCOLOR	Couleur du texte du bouton	black
FONTTYPE	Famille de police	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. 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 support.ecom@ingenico.com (uniquement pour les comptes de production puisque c'est une option payante ! Activez l'option « Logo Hosting » avant de nous envoyer votre logo).</p> <p>Si le logo est enregistré sur nos serveurs, l'URL sera https://secure.ogone.com/images/merchant/[PSPID]/[image]</p>	-

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.

### 6.1.1 Hébergement de logo

Afin de vous conformer aux PCI-DSS (2015) le plus récent, vous êtes tenu d'héberger vos images (et tout autre support utilisé sur la page de paiement) dans un environnement avec la certification PCI la plus élevée.

Ogone ayant exactement ce type d'environnement sécurisé, nous vous recommandons d'héberger vos fichiers chez nous à l'aide de [File Manager](#) (Gestionnaire de fichiers) sur votre compte Ogone. File Manager (Gestionnaire de fichiers) est une fonctionnalité (gratuite) qui vous permet de télécharger et de gérer facilement et efficacement vos fichiers modèles.

Pour renvoyer vers le logo téléchargé, il vous suffit de saisir le nom du fichier dans le champ « LOGO » de votre formulaire de commande.

Vous pouvez également envoyer votre logo (fichier .jpg, .png ou .gif) avec votre PSPID à support.ecom@ingenico.com. Toutefois, cette option étant payante (!), cela n'est possible que pour les comptes de production. Avant de nous envoyer votre logo, veuillez activer l'option « "Logo Hosting" » (Hébergement de logo) sur votre compte : « Configuration » > « Compte » > « Vos options ».

Pour renvoyer vers le fichier téléchargé, vous devez saisir l'URL absolue dans le champ « LOGO » sur votre formulaire de commande en suivant la structure suivante : https://secure.ogone.com/images/merchant/[PSPID]/[image]

#### Important

Il n'est pas possible d'utiliser des fichiers précédemment téléchargés par Ogone en même temps que des fichiers téléchargés avec « File Manager » dans votre intégration. Par conséquent, si vous avez des fichiers qui ont été précédemment téléchargés par Ogone, veuillez vous assurer de télécharger une nouvelle fois ces fichiers vous-même à l'aide de « File Manager ».

## 6.2 Modèle hébergé par Ogone (modèle statique)

En utilisant un modèle sur la page de paiement hébergée, vous pouvez personnaliser sa conception de façon beaucoup plus évoluée que si vous utilisez simplement vos champs de logo, de titre et de couleur.

Vous concevez totalement votre propre page de modèle, en y laissant simplement une section destinée à être complétée par notre



système.

Vous hébergez votre page et vos fichiers de modèle sur notre environnement sécurisé, sous la forme de ce que nous appelons un "modèle statique".

### 6.2.1 Champs cachés

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	Nom de fichier du modèle hébergé par Ogone.

Exemple:

```
<input type="hidden" name="TP" value="mytemplatefile.html">
```

### 6.2.2 Zone de paiement (Payment zone)

Vous pouvez concevoir l'ensemble du modèle de page 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\$\$\$.

### 6.2.3 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.

table.ncoltable1		<b>My Webshop</b>	
		Order Reference : STDREF123	td.ncoltxttr
td.ncoltxtl	Total Charge : 1.00 EUR		
Beneficiary : Consulting SA			

table.ncoltable2		Please select a payment method by clicking on the logo		td.ncolhl
Card: SSL secured transaction		 		

table.ncoltable3					
 		Our Logo			
td.ncollogo		<a href="#">About</a>   <a href="#">Privacy Policy</a>   <a href="#">Security</a>		input.ncol	

Pay with : 	
td.ncoltxtl2	Card holder's name* : Bill Smith
Card number* : <input type="text"/>	
td.ncolinput	
Expiry date (mm/yyyy)* : <input type="text"/> / <input type="text"/>	
Card verification code * : <input type="text"/> CVC present <input type="checkbox"/> <a href="#">What is this ?</a>	
*** Mandatory fields.	
input.ncol	<input type="button" value="Yes, I confirm my order"/>

<b>Your payment is authorised</b>	
td.ncoltxtc	Payment reference :1248886

### 6.3 Mise en page basée sur le modèle (modèle dynamique)

La page de modèle dynamique vous permet de personnaliser la conception des pages de paiement de façon plus évoluée qu'avec le modèle statique.

Lorsque vous utilisez une page de modèle dynamique, vous concevez totalement votre propre page de modèle, en y laissant simplement une section destinée à être complétée par notre système. L'adresse URL de votre page de modèle doit nous être envoyée dans les champs cachés pour chaque transaction.

Veuillez garder à l'esprit que le fait d'utiliser une page de modèle dynamique implique une demande supplémentaire auprès de notre système pour consulter votre page de modèle. Ceci accroît le temps nécessaire au processus de paiement.

### Important

Pour rester en conformité avec la dernière version de PCI-DSS, vous devez héberger votre modèle (et les fichiers associés) dans un environnement ayant la plus haute certification PCI. Si cela n'est pas à votre portée, nous vous conseillons vivement d'héberger vos fichiers de modèles avec Ogone, en utilisant un [modèle statique](#) et notre [gestionnaire de fichiers](#) (Template File Manager). N'oubliez pas toutefois que dans ce cas, votre modèle peut perdre une partie de son [comportement dynamique](#) (en fonction de votre intégration).

### 6.3.1 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 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 doit aussi avoir un URL absolu.

### 6.3.2 Zone de paiement (Payment zone)

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\$\$\$.

Vous trouverez un exemple de modèle de page dynamique à l'adresse suivante : [https://secure.ogone.com/ncol/template\\_standard.htm](https://secure.ogone.com/ncol/template_standard.htm)

### 6.3.3 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=...

### 6.3.4 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.ncolxtl {background-color : #ffffcc; color : black; text-align : right; font-weight : bold}
td.ncolxtl2 {background-color : #ffffcc; color : black; text-align : right; font-weight : bold}
td.ncolxtlr {background-color : #ffffcc; color : black; text-align : left; font-weight : bold}
td.ncolxtc {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.

table.ncoltable1		<b>My Webshop</b>	
td.ncoltxt1		Order Reference : STDREF123	td.ncoltxttr
		Total Charge : 1.00 EUR	
		Beneficiary : Consulting SA	







table.ncoltable2		Please select a payment method by clicking on the logo		td.ncolhl
		Card: SSL secured transaction		
		 		

table.ncoltable3					
 		Our Logo			
td.ncollogo		<a href="#">About</a>   <a href="#">Privacy Policy</a>   <a href="#">Security</a>		input.ncol	

Pay with : 	
td.ncoltxt12	Card holder's name* : Bill Smith
	Card number* : <input type="text"/>
	Expiry date (mm/yyyy)* : <input type="text"/> / <input type="text"/>
	Card verification code * : <input type="text"/> CVC present <input type="text"/> <a href="#">What is this ?</a>
*** Mandatory fields.	
input.ncol	<input type="button" value="Yes, I confirm my order"/>

td.ncoltxtc		<b>Your payment is authorised</b>	
		Payment reference :1248886	

### 6.3.5 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.

Nous nous ferons un plaisir de modifier cette temporisation (HTTPTimeOut) de notre côté sur demande du marchand (via un ticket d'assistance).

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 Ogone.

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 équipe commerciale pour trouver une solution si vos volumes de transaction sont importants.

## 6.4 Modèle pour mobile

Vous pouvez optimiser l'affichage de la page paiement sur les appareils mobiles (smartphones, tablettes, etc.) en appliquant une page de modèle, assortie de feuilles de style, comme expliqué dans les chapitres suivants.

### 6.4.1 Paramètres de présentation

Les champs ci-dessous peuvent être personnalisés en indiquant certaines informations dans la requête :

```
<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	Description	Valeur par défaut
TITLE	Titre de la page	Title
BGCOLOR	Couleur de fond	white
TXTCOLOR	Couleur de texte	black
TBLBGCOLOR	Couleur d'arrière-plan des colonnes de droite	white
TBLTXTCOLOR	Couleur du texte des colonnes de droite	black
BUTTONBGCOLOR	Couleur de fond des boutons	s.o.
BUTTONTXTCOLOR	Couleur du texte des boutons	black
LOGO	URL/nom de fichier du logo que vous souhaitez afficher sur la page de paiement  <a href="https://secure.ogone.com/images/merchant/[PSPID]/[image]">https://secure.ogone.com/images/merchant/[PSPID]/[image]</a>  Important : La nouvelle norme PCI-DSS de 2015 indique que vos logos et autres images figurant sur la page de paiement doivent être hébergés sur Ogone.	-
FONTTYPE	Famille de la police	Verdana

### 6.4.2 Modèle

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

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

Champ	Description
TP	<p>URL de la page de modèle dynamique. L'URL doit être absolue (contenir le chemin complet), elle ne peut pas être relative. Tout élément inclus dans la page de modèle doit également avoir une URL absolue.</p> <p><b>Important :</b> Conformément aux exigences PCI-DSS (2015) les plus récentes, vous devez héberger les éléments de modèle utilisés sur la page de paiement dans un environnement avec la certification PCI la plus élevée. Par conséquent, nous vous recommandons d'héberger vos fichiers avec Ogone, en utilisant <a href="#">File Manager</a>.</p>

#### Zone de paiement

La page de modèle peut être personnalisée entièrement. Seule obligation : elle doit comporter la chaîne « \$\$\$PAYMENT ZONE\$\$\$ », qui indique l'emplacement où notre e-Commerce module peut ajouter son champ dynamiquement. Elle doit donc au moins contenir les éléments suivants :

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

Accédez aux [exemples de modèles](#) et utilisez les modèles que nous avons créés, ou inspirez-vous de nos modèles pour créer le vôtre.

### 6.4.3 Feuilles de style (CSS)

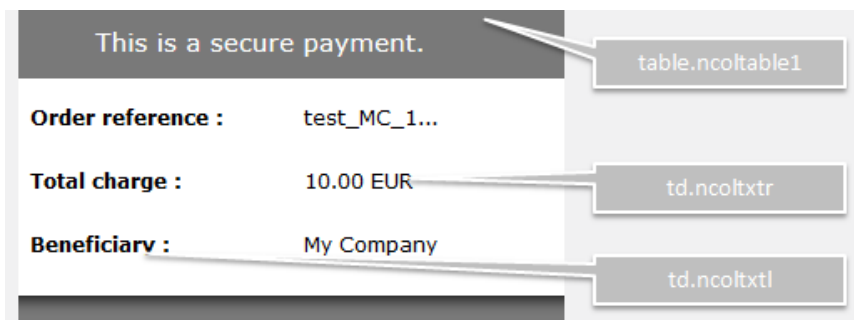
Pour mieux gérer et comprendre le CSS, nous avons divisé le CSS du modèle en quatre parties principales :

- [En-tête](#)
- [Informations de paiement](#)
- [Pied de page](#)
- [Section du statut de paiement](#)

**Remarque :** Bien que les exemples d'images ci-dessous reflètent les éléments qui seront affectés par le CSS, le style (couleurs, images, etc.) utilisé peut différer de ce qui est indiqué dans les exemples de codes associés.

#### [En-tête](#)

Ce style vous permet de modifier l'en-tête de la page de paiement comme indiqué ci-dessous :



Élément(s)

- Partie verrouillée

```
.securedBG
{
background: #797979;
}
.secured
{
padding: 8px 20px 0px 40px;
color: #ffffff;
width: 235px;
margin: 0 auto;
background: url("lock.png") 5px no-repeat #797979;
height: 30px;
}
```

- Récapitulatif de la commande

```
table.ncoltable1
{
width: 100%;
margin: 0 auto;
min-width: 300px !important;
}
td.ncoltxtl
{
font-family: open-sans ,Verdana,sans-serif;
font-size: 14px;
background-color:#ffffff;
text-align : left !important;
font-weight : bold !important;
vertical-align:bottom;
}
td.ncoltxtr
{
text-align: left;
font-weight: normal;
font-family: open-sans ,Verdana,sans-serif;
```



```
font-size: 14px;  
background-color:#ffffff;  
}
```

### Informations de paiement

Ce style vous permet de personnaliser la section des informations de paiement comme indiqué ci-dessous :

The image shows a payment form with the following elements and their corresponding labels:

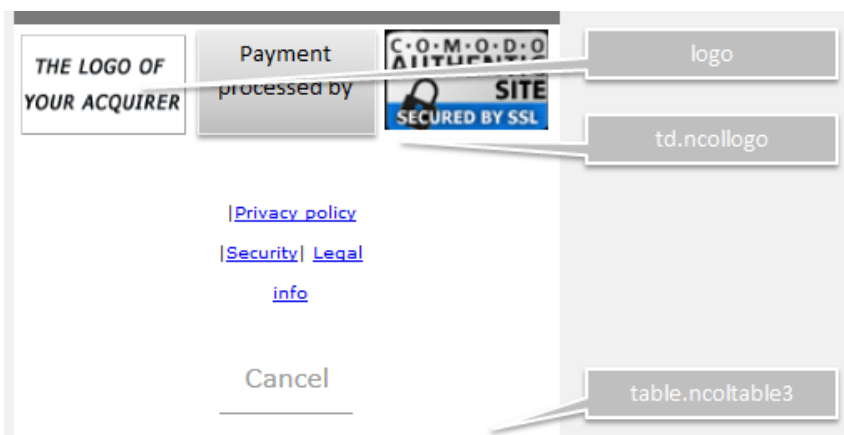
- Pay with :** Labeled with `table.ncoltable2`.
- Cardholder's name\* :** Labeled with `td.ncoltxt2`.
- Card number\* :** Labeled with `td.ncolinput`.
- Expiry date (mm/yyyy)\* :** Labeled with `td.ncolinput`.
- Card verification code\* :** Labeled with `td.ncolinput`.
- What is this?** Labeled with `td.ncolinput`.
- \* Mandatory fields** Labeled with `td.ncolinput`.
- Yes, I confirm my payment** Labeled with `input.ncol`.

```
td.ncolinput  
{  
text-align: left;  
font-weight: normal;  
font-size: 14px;  
font-family: open-sans ,Verdana,sans-serif;  
display: block;  
box-shadow: none !important;  
}
```

```
input.ncol
{
background-color: #ffffff;
height: 40px;
font-size: 14px;
text-align: center;
padding: 0px;
font-family: open-sans ,Verdana,sans-serif;
margin: 0 35px 20px;
border-bottom: 1px solid #999999;
border-radius: 0px;
-webkit-appearance: none !important;
-webkit-border-radius: 0 !important;
}
td.ncolxtl2
{
text-align: left;
font-family: open-sans ,Verdana,sans-serif;
white-space: nowrap;
display: block;
font-size: 14px;
background-color:#ffffff;
}
```

### Pied de page

Ce style vous permet de modifier le pied de page de la page de paiement :



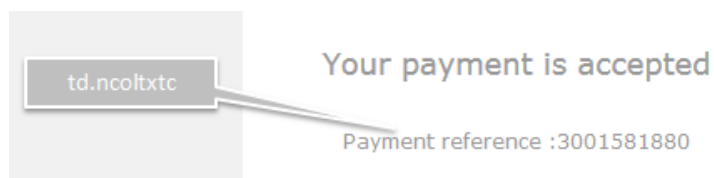
### Élément(s)

```
td.ncollogoc
{
text-align: center;
font-weight: normal;
```

```
font-size: 14px;
padding: 2px;
vertical-align: top !important;
}
td.ncollogoc IMG
{
width: 90px;
height: 55px;
margin-right: 4px;
}
.ncollogoc td .ncol
{
width: auto;
padding-right: 10px;
padding-left: 10px;
cursor:pointer;
}
.ncollogoc input.ncol
{
margin-top:10px !important;
-webkit-appearance: none !important;
-webkit-border-radius: 0 !important;
}
```

### Section du statut de paiement

Cette section vous permet de personnaliser la présentation de la page du statut de paiement) comme indiqué ici :



#### Élément(s)

```
td.ncoltxtc
{
background-color:#ffffff;
color:#999999;
padding: 0px;
text-align: left;
font-weight: normal;
font-size: 14px;
border-top: 0px solid #ffffff;
font-family: open-sans ,Verdana,sans-serif;
}
td.ncoltxtc h3
```

```
{
text-align: center;
font-weight: normal !important;
padding: 5px;
font-family: open-sans ,Verdana,sans-serif;
}
td.ncoltxtmessage
{
background-color: #ffffff;
color: #999999;
text-align: left;
font-weight: normal;
}
```

Voici ce à quoi la page doit ressembler :


This is a secure payment.

Order reference :test\_MC\_1...

Total charge :10.00 EUR

Beneficiary :My Company

Pay with :



Cardholder's name\* :

Card number\* :

Expiry date (mm/yyyy)\* :

08

/

2024

Card verification code\* :


What is this?

\* Mandatory fields

Yes, I confirm my payment

THE LOGO OF  
YOUR ACQUIRER

Payment  
processed by



[Privacy policy](#)

[Security](#) [Legal](#)

[info](#)

table.ncoltable1

td.ncoltxtr

td.ncoltxtl

table.ncoltable2

td.ncoltxt2

td.ncolinput

input.ncol

td.ncollogo

6.4.4 Exemples de pages

Pour vous aider à démarrer, nous avons créé ces pages.

La première est une version de marque que vous pouvez utiliser comme exemple :

<https://secure.ogone.com/ncol/StandardMobileTemplate.htm>

Vous pouvez aussi utiliser la version « dénudée » ci-après comme base pour créer votre propre modèle :

[https://secure.ogone.com/ncol/StandardMobileTemplate\\_generic.htm](https://secure.ogone.com/ncol/StandardMobileTemplate_generic.htm)

Ces deux modèles ainsi que d'autres fichiers (polices, images) sont disponibles au format compressé [ici](#)

## 6.5 Gestionnaire de fichiers modèles

Avec le « Gestionnaire de fichiers modèles », vous pouvez facilement gérer vos modèles et les différents fichiers connexes.

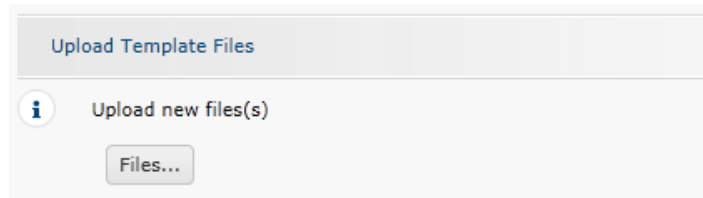
Pour commencer à utiliser le « Gestionnaire de fichiers », connectez-vous à votre compte Ogone et allez dans « Configuration » > « Modèle » > « Gestionnaire de fichiers ».

### Important

Il n'est pas possible d'utiliser des fichiers précédemment téléchargés par Ogone en même temps que des fichiers téléchargés avec le « Gestionnaire de fichiers » dans votre intégration.

Par conséquent, si vous avez des fichiers qui ont été précédemment téléchargés par Ogone, veuillez vous assurer de télécharger une nouvelle fois ces fichiers vous-même à l'aide de « Gestionnaire de fichiers ».

### 6.5.1 Télécharger des fichiers modèles



Dans « Télécharger des fichiers modèles », sélectionnez le bouton « Fichiers... » pour parcourir les fichiers que vous voulez télécharger. Vous pouvez télécharger des Javascripts, des fichiers html et css et des images (.css, .jpg, .jpeg, .gif, .png, .html, .js), avec un maximum de 7 Mb par fichier, et 10 Mb au total.



Faites votre sélection puis confirmez.


### 6.5.2 Contrôler et gérer les fichiers téléchargés


Une fois le téléchargement terminé, vous verrez vos fichiers téléchargés sur la même page dans la partie « Fichiers téléchargés ».


Le statut des fichiers sera d'abord « En cours de validation ». Pendant ce temps, plusieurs contrôles de sécurité/virus sont réalisés.

Vous pouvez utiliser les fichiers lorsque leur statut est « Validé ».

Cliquez sur le bouton « Actualiser »  pour vérifier le statut de vos fichiers / Cliquez sur le bouton « Supprimer »  pour supprimer définitivement le fichier.









 For creating a template, you reference your resources with the following code: "\$\$\$TP RESOURCES URL\$\$\$/[your file name]".

 The file name of the template must be passed as parameter "TP" value to use chosen static template.

 For using an uploaded image file as your logo on the payment page, send the LOGO parameter with your image filename as value.

Q

Drag "File Type" or "Status" column header and drop it here to group by that column

File Name	File Type	Size	Status	Upload Date	Action
successful_top.png	Image	4KB	Validating 	2015-07-08 10:13:16	
4ec6d8b8-2af4-4279-bfdc-7fe40dfaf9e6_6.jpg	Image	2035KB	Validated 	2015-06-25 15:52:45	
layer_styling_v5.css	CSS	9KB	Validated 	2015-06-22 14:53:16	
cancel_top.png	Image	2KB	Validated 	2015-06-16 15:55:09	

Un fichier aura le statut « Refusé » s'il ne passe pas le contrôle de sécurité. Cela peut être dû à la présence d'un virus ou à une extension de fichier erronée, par exemple.

### 6.5.3 Intégration

Dans vos modèles, vous renvoyez vers vos fichiers téléchargés avec un code en respectant la structure suivante : \$\$\$TP RESOURCES URL\$\$\$/[nom de votre fichier].

Exemple :

```
<html>
<head>
  <title>Great Shop Test Page</title>
  <link rel="stylesheet" type="text/css" href="$$$TP RESOURCES URL$$$/layer_styling_v5.css">
  <script src="$$$TP RESOURCES URL$$$/test.js"></script>
</head>
<body>
  <div>Great Shop Template</div>
  <div>$$$PAYMENT_ZONE$$$</div>
  
</body>
</html>
```

Pour renvoyer vers le modèle que vous avez téléchargé dans votre intégration e-Commerce, vous envoyez le nom du fichier modèle avec le paramètre « TP ».

Exemple : TP=mytemplatefile.html

Lorsque vous avez une intégration de base e-Commerce au moyen d'un logo en haut de la page, vous devez renvoyer vers le logo téléchargé en envoyant le nom du fichier avec le paramètre « LOGO » (LOGO).

Exemple : LOGO=mycompanylogo.png

## 6.6 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 "Modèle", 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 Ogone 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 Ogone par défaut qui sera utilisé.

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 notre service clientèle), 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 Contrôle 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.

## 6.7 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).

### 6.8 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 des inconvénients :

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

Pour ces raisons, Ogone déconseille formellement l'utilisation des iframes, et leur utilisation est aux risques et périls du marchand. Nous recommandons l'utilisation de Modèles Dynamiques comme alternative.

Si vous souhaitez tout de même utiliser un iframe, veuillez noter les recommandations suivantes :

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

## 7. Retour d'information sur la transaction

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.

### 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 [Requête de réponse directes \(après paiement\)](#)).

Dans votre compte Ogone, naviguez vers "Configuration" > "Information technique" > "Retour d'information sur la transaction". Veuillez configurer les paramètres comme décrit ci-dessous. :

Redirection HTTP dans le navigateur :

☒ I would like to receive transaction feedback parameters on the redirection URLs.

("Je veux recevoir les paramètres de transaction en retour dans les URL lors de la redirection.")

Requête directe HTTP serveur-à-serveur :

#### Direct HTTP server-to-server request



##### Timing of the request

- ☐ No request.
- ☒ Always deferred (not immediately after the payment).
- ☐ Always online (immediately after the payment to allow customisation of the response seen by the customer).
- ☐ Online but switch to a deferred request when the online requests fail.

("Toujours en background/différé (pas tout de suite après le paiement).")

### 7.1 Réaction par défaut

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

HTTPS://OUR URL/order\_Agree.asp

## My webshop

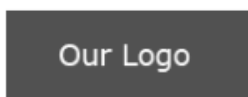
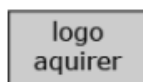
Order reference : STDREF789

Total charge : 1.00 EUR

Beneficiary : Webshop

## Authorised

Payment reference :15987181



[About](#) | [Privacy policy](#) | [Security](#) | [Legal info](#)



[Back to merchant site](#)

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.

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 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.<br><br>Lorsque vous envoyez la valeur « NONE » (néant), le bouton ramenant le client au site du marchand est masqué. |

## 7.2 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.

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).<br>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).<br>Si ce champ est vide, le declineurl sera présenté au client en lieu et place.                              |

### 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 Ogone 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. »)

## 7.3 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. »

### 7.3.1 SHA-OUT

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 la [Paramètres à inclure dans le calcul SHA-OUT](#).

Veuillez noter que ces valeurs sont toutes sensibles à la casse.

### Important

- Tous les paramètres envoyés (et qui apparaissent dans la liste [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)

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 s'assurer de l'exactitude et de l'intégrité des valeurs de paramètre envoyées dans la requête.

### Exemple d'un calcul SHA-1-OUT élémentaire

Paramètres :

ACCEPTANCE: 1234

amount: 15

BRAND: VISA

CARDNO: XXXXXXXXXXXX1111

currency: EUR

NCERROR: 0

orderId: 12

PAYID: 32100123

PM: CreditCard

STATUS: 9

Clé SHA-OUT :

Mysecretsig1875!?

Chaîne entière à hacher :

ACCEPTANCE=1234Mysecretsig1875!?AMOUNT=15Mysecretsig1875!?BRAND=VISAMysecretsig1875!?

CARDNO=XXXXXXXXXXXX1111Mysecretsig1875!?CURRENCY=EURMysecretsig1875!?NCERROR=0

Mysecretsig1875!?ORDERID=12Mysecretsig1875!?PAYID=32100123Mysecretsig1875!?PM=CreditCard  
Mysecretsig1875!?STATUS=9Mysecretsig1875!?

Condensé obtenu (SHA-1) :

209113288F93A9AB8E474EA78D899AFDBB874355

#### Encodage des caractères pour les méthodes de paiement PostFinance

Si vous utilisez l'encodage par caractères UTF-8 pour l'intégration de PostFinance Card et/ou de PostFinance E-finance, la réponse de la transaction sera envoyée selon l'encodage par caractères ISO-8859-1.

## 7.4 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).

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](#).

### 7.4.1 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.

#### URL d'après-paiement variables pour plusieurs shops

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="">
```

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>

Important: Ne pas utiliser de caractères spéciaux dans le champ de PARAMVAR, car ils seront codées URL, ce qui pourrait créer des liens non valides..

### 7.4.2 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 :

Dans ce cas, notre système n'enverra pas de requête. Cette option vous permet de désactiver vos URL d'après-paiement en cas de maintenance ou de problèmes sur votre serveur.

- 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](#)).

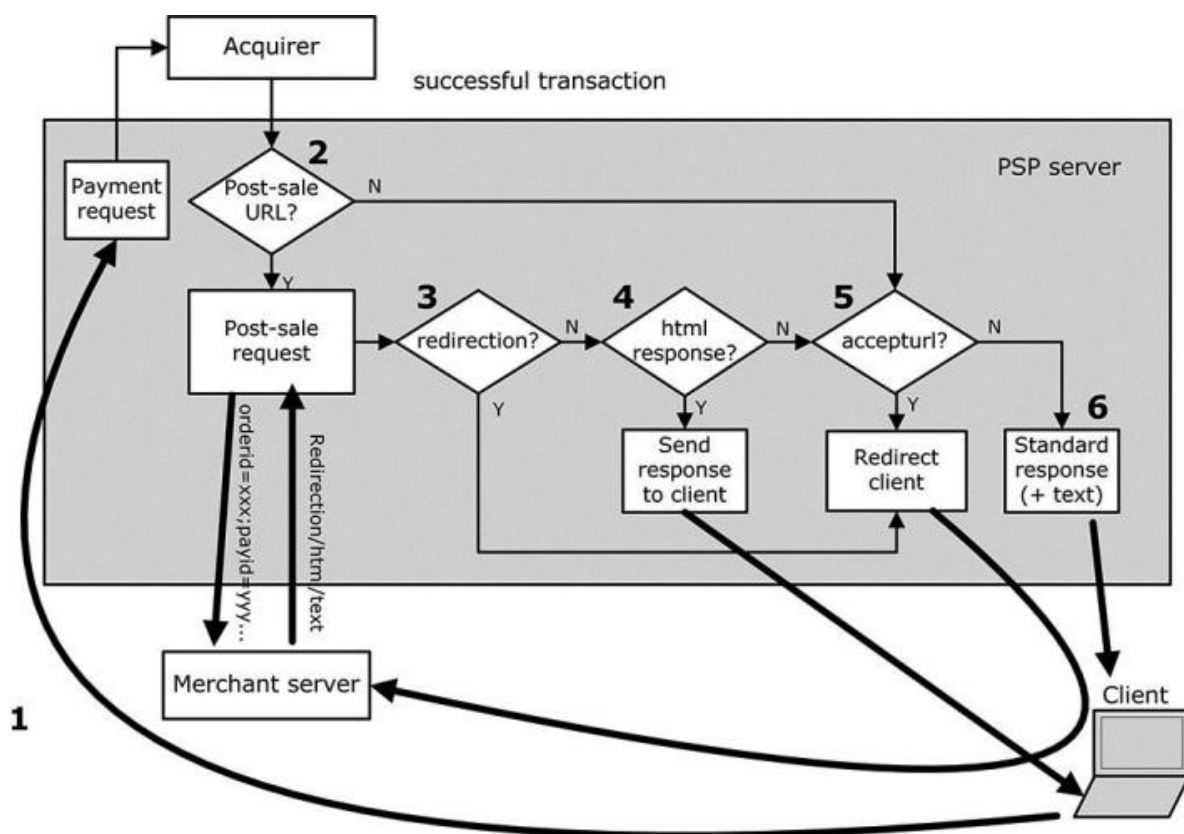
### 7.4.3 Réponse envoyée au client

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 depending on transaction result](#)).

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](#)).

Le diagramme présenté ci-dessous illustre le processus qui intervient au terme d'une transaction en cas d'autorisation ou d'acceptation du paiement dans le cadre d'une demande d'informations après paiement en ligne. (Lorsque le paiement est annulé, refusé ou incertain, le processus est similaire mais le système utilise alors les « CANCELURL » / « DECLINEURL » / « EXCEPTIONURL » et les pages « cancellation/rejection »).



#### 7.4.4 Requête http pour les changements de statut

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).



## 7.5 Paramètres du retour d'information

Lorsqu'un paiement est exécuté, nous pouvons envoyer la liste de paramètres suivants:

| Paramètre  | Valeur   |
|------------|--|
| ACCEPTANCE | Code d'acceptation produit par l'acquéreur   |
| amount     | Montant de la commande (pas multiplié par 100)                                       |
| BRAND      | Marque de la carte (notre système se base pour cela sur le numéro de carte)          |
| CARDNO     | Numéro masqué de la carte  |
| CN         | Nom du titulaire de la carte/client  |
| currency   | Devise de la commande  |
| ED         | Date d'expiration  |
| NCERROR    | Code d'erreur  |
| orderId    | Votre référence de commande  |
| PAYID      | Référence du paiement dans notre système   |
| PM         | Moyen de paiement  |
| SHASIGN    | Signature SHA calculée par notre système (si configuré sur <a href="#">SHA-OUT</a> ) |
| STATUS     | Statut de la transaction   |
| TRXDATE    | Date de la transaction   |

### Exemple (GET request):

`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`

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.

### 7.5.1 Paramètres du retour d'information dynamiques

Vous pouvez également choisir quels paramètres sont envoyés avec la requête post-paiement. Pour faire ceci, rendez-vous dans l'onglet "Retour d'information sur la transaction" de votre information technique. Il y a là une liste de paramètres "Disponible" et "Sélectionné".

Utilisez tout simplement les flèches entre les deux listes pour faire basculer les paramètres d'une liste à l'autre.

N'oubliez pas de mettre à jour votre signature SHA-OUT afin de tenir compte des paramètres indiqués ici. Les paramètres qui ne sont pas sélectionnés ne figureront PAS dans le calcul SHA.

### 7.5.2 Paramètres du retour d'information

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 | <p>Champ servant à soumettre certains paramètres et leurs valeurs que vous aimeriez récupérer dans la demande d'informations.</p> <p>Le champ paramplus n'est pas inclus dans les paramètres des informations proprement dits ; les paramètres/valeurs que vous soumettez dans ce champ seront en revanche analysés et les paramètres ainsi obtenus, ajoutés à la demande http.</p> |

#### 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?[...standard.parameters...]
```

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

### 7.6 Réinitialisation du retour d'information

Si la demande de redirection/retour d'information n'a pas été exécutée, du fait d'une action du client entraînant le blocage de nos pages de paiement sécurisé (par ex. si le client a cliqué sur le bouton « retour » de son navigateur), nous pouvons réinitialiser la demande de post-paiement et/ou la redirection. Ainsi, votre client sera redirigé vers la page que vous souhaitez afficher et vos bases de données pourront être mises à jour.

Pour activer cette fonction dans votre compte, allez dans Configuration > Information technique > Retour d'information sur l... > Général et cochez la case "Je veux que Ogone relance le processus de fin de transaction (requête/redirection post paiement) si nécessaire."

Il est possible que vous receviez plusieurs demandes de post-paiement pour le même identifiant de commande. En effet, la demande de redirection/retour d'information sera renvoyée si le client revient aux pages de paiement sécurisé à l'aide du bouton « retour » après avoir été redirigé vers votre site web.

Veillez à configurer votre script « Post URL » de façon à traiter ces « exceptions ». Par exemple, vous pouvez configurer votre script « Post URL » de manière à créer une ligne dans votre base de données pour chaque état de transaction renvoyé et/ou générer un e-mail pour

informer le marchand d'une « exception » par rapport aux étapes prévues dans le processus de transaction.

Nous vous recommandons de ne pas écraser le premier message d'état de transaction que vous recevez par un autre message reçu par la suite pour le même identifiant de commande. Idéalement, il est conseillé de conserver toutes les réponses pour chaque commande, et d'appeler un processus permettant de les analyser et de les traiter comme il se doit.

Si vous ne cochez pas la case, le client qui clique sur le bouton « retour » pour revenir aux pages de paiement sécurisé verra s'afficher un message indiquant que le paiement a déjà été traité.

## 7.7 E-mails de confirmation

### 7.7.1 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.

### 7.7.2 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 courriels 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 |

## 8. e-Commerce via 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://secure.ogone.com/ncol/test/orderstandard.asp / orderstandard\\_utf8.asp?PSPID=TESTSTD&orderId=order123&amount=12500&currency=EUR&SHASIGN=8DDF4795640EB9FE9B367315C48E47338129A4F5& ...](https://secure.ogone.com/ncol/test/orderstandard.asp/orderstandard_utf8.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.

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

- Le champ référent/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 au chapitre [SHA-IN Signature](#).

## 9. Moyen de paiement et caractéristiques de la page de paiement

### 9.1 Choix du moyen de paiement du côté du marchand

#### 9.1.1 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'acceptons 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 (par ex. CreditCard)      |
| BRAND | Marque de la carte de crédit (par ex. VISA) |

#### 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="">
```

OU

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

#### 9.1.2 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 pages 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 ».

Remarque: 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. |

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.

## 9.2 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). |

### Exemple

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">
```

### 9.3 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). |

### 9.4 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 | <p>Les valeurs possibles sont 0, 1 et 2.</p> <ul style="list-style-type: none"> <li>0 : Logos regroupés horizontalement avec le nom du groupe sur la gauche (valeur par défaut)</li> <li>1 : Logos regroupés horizontalement sans les noms des groupes</li> <li>2 : Liste verticale de logos avec moyen de paiement et nom de la marque</li> </ul> |

### 9.5 Fenêtre pour 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.

Ce champ masqué est le suivant :

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

| Champ  | Valeurs possibles  |
|--------|--|
| WIN3DS | <ul style="list-style-type: none"> <li>« MAINW » : pour afficher la page d'identification dans la fenêtre principale (valeur par défaut)</li> <li>« POPUP » : pour afficher la page d'identification dans une fenêtre contextuelle (pop-up) et revenir à la fenêtre principale à la fin</li> </ul> |

#### 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.

### 9.6 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)<br>"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 Ogone. Accédez à [Subdivision en cartes de crédit/débit](#) pour plus d'informations.



## 10. Autres champs masqués facultatifs

### 10.1 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 | <p>Code d'opération pour la transaction.</p> <p>Valeurs possibles pour les nouvelles commandes :</p> <ul style="list-style-type: none"> <li>• RES : demande d'autorisation</li> <li>• SAL : demande de vente (paiement)</li> </ul> <p>Optionnel:</p> <ul style="list-style-type: none"> <li>• PAU: demande de pré-autorisation:<br/>           En accord avec votre acquéreur vous pouvez utiliser ce code d'opération pour réserver temporairement des fonds sur la carte d'un client. Ceci est une pratique courante dans les industries liées au voyage et à la location. Le code PAU/pré-autorisation ne peut actuellement être utilisé que pour les transactions MasterCard et n'est supporté que par quelques acquéreurs. Ce code d'opération ne peut pas être défini comme valeur par défaut dans votre compte Ogone.<br/>           Si vous deviez utiliser le code PAU pour des transactions avec des acquéreurs ou des types de carte qui ne supportent pas la pré-autorisation, ces transactions ne seraient pas bloquées, mais traitées comme des autorisations classiques (RES).</li> </ul> |

Afin que ce paramètre 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 au chapitre [Signature SHA-IN](#).

### 10.2 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 |

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).