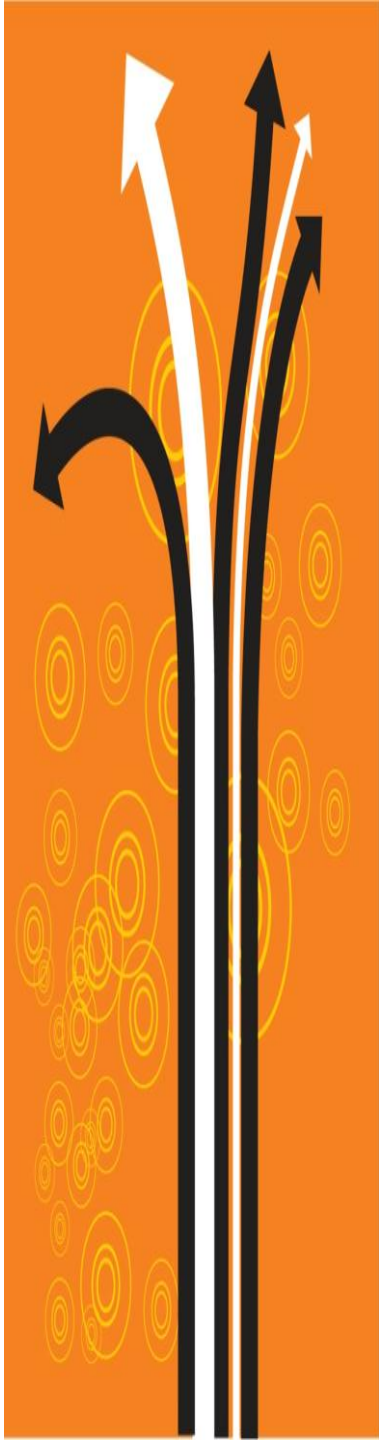
Orange Money

Paiement internet

API d'intégration page de paiement



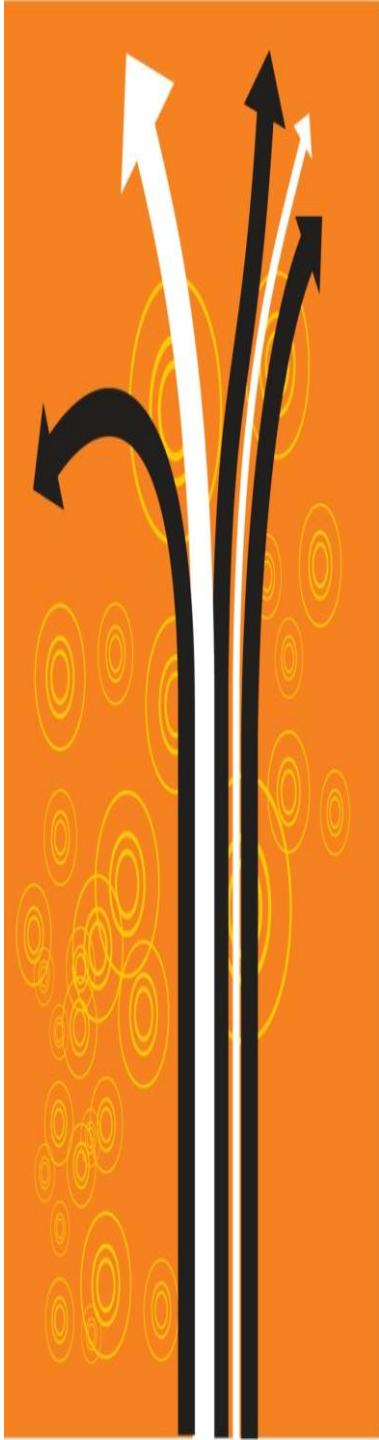
sonatel

Sonatel Multimédia - Septembre 2015

orange™

SOMMAIRE

sonatel



1. Présentation du système

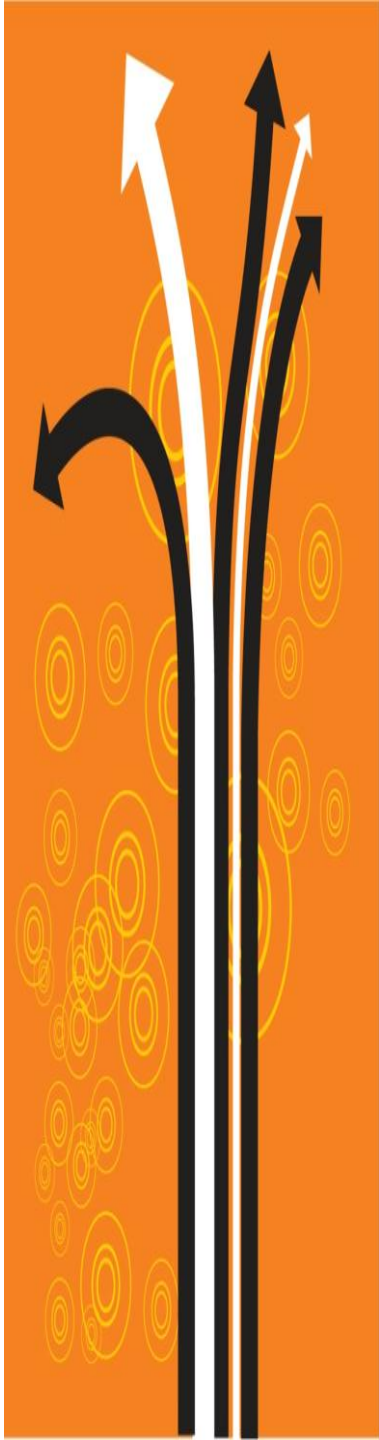
Le système de paiement par Orange Money sur internet est une page de paiement sécurisée en redirection hébergée sur les serveurs de Sonatel.

Il s'interface avec tout type de site marchand internet ou mobile.

Lorsqu'un acheteur initie l'action de paiement sur le site marchand intégrant ce système, il est redirigé automatiquement vers la page de paiement distante Orange Money.

Cette page est personnalisable pour permettre de garantir une certaine cohérence avec l'identité visuelle du site marchand.

2. Sécurité



sonatel

orange™

2.1 Identification

Pour utiliser l'API, il faut disposer d'un compte sur le système.

Un site marchand est identifié par deux éléments:

- ✓ Un identifiant partenaire
- ✓ Un identifiant site marchand

Ces deux paramètres sont fournis lors de l'inscription du commerçant au service de paiement Orange Money sur internet.

Ils sont obligatoires dans tous les messages envoyés sur notre plateforme par le site marchand.

Une interface d'administration est également mise à disposition des partenaires afin de personnaliser leur espace de paiement et suivre les détails de leurs transactions par site marchand; seul l'identifiant partenaire est requis pour l'accès à cette interface.

2.2 Authentification

Pour accéder à la plateforme de paiement Orange Money, le site marchand doit apporter la preuve de son identité.

Pour cela, et afin de garantir la sécurité des transactions, chaque site marchand est authentifié par une clé de sécurité secrète.

Cette clé, qui ne doit être connue que du site marchand et du système, doit être générée par le commerçant lui même via son espace personnel.

La clé secrète servira à signer tous les messages échangés entre le site marchand et les serveurs de paiement Orange Money et ainsi assurer que la demande de paiement provient d'une source identifiée et authentifiée.

2.2.1 Gestion de la clé d'authentification (suite)

a) Génération

Afin de pouvoir utiliser l'API de paiement, le commerçant doit au préalable générer sa clé secrète.

La fonctionnalité est disponible sur le backoffice commerçant, onglet « Gestion clé de sécurité », menu « Générer ».

Le commerçant doit saisir une phrase secrète et appuyer sur le bouton « valider ». *Un indicateur de complexité indiquera le niveau de complexité de la phrase secrète et le bouton « valider » apparaitra dès la clé sera jugée assez robuste.*

Une fois votre clé secrète générée, le commerçant a la charge de la garder en lieu sûr. Les clés secrètes ne sont ni envoyées par mail, ni restituter.

En cas de perte de la clé secrète, il faudra en générer une autre en utilisant le même procédé que celui décrit plus haut.

2.2.1 Gestion de la clé d'authentification (suite)

b) Validation

Toute génération de clé secrète doit être validée par le commerçant.

Un mail de confirmation est envoyé à l'adresse fourni par le commerçant à la souscription au service.

En aucune façon le mail ne contiendra la clé secrète, mais un mail de confirmation qui basculera le commerçant vers son espace personnel.

2.2.1 Gestion de la clé d'authentification (suite)

c) Expiration

Pour des raisons de sécurité, la clé secrète est valable 90 jours.

Passé ce délai, une alerte apparaitra sur l'espace personnel du commerçant.

L'expiration de la clé secrète n'interrompt pas l'accès au service de paiement pour ne pas entraver l'activité du site marchand. Elle sera tout de même rappelée sur l'interface personnelle, ceci pour la sécurisation des transactions.

2.2.1 Gestion de la clé d'authentification (suite)

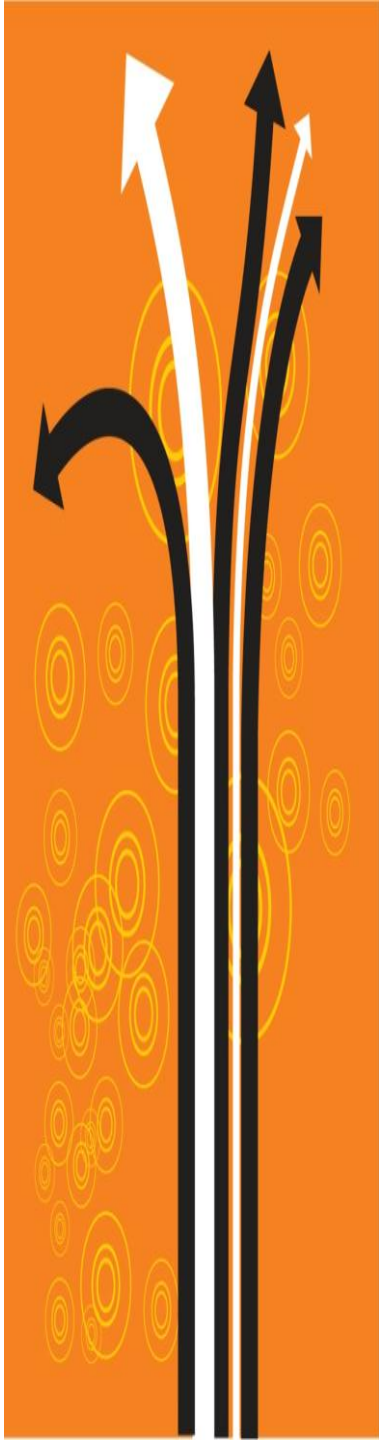
d) Sécurisation

Une fois générée, la clé secrète n'est plus affichée sur l'interface, ni demandée par le système.

Il ne sera donc jamais demandé au commerçant dans aucune correspondance, ni par mail, courrier ou téléphone.

Elle doit être gérée avec prudence et stockée en lieu sûr.

3. Intégration de l’API



sonatel

orange™

3.1 Description

L'intégration du système de paiement par Orange Money sur un site marchand se fait simplement par l'envoi d'une requête HTTPS de type POST, avec un certain nombre de paramètres (décrits plus bas), vers le serveur de paiement Orange Money.

L'acheteur bascule ainsi sur la page de paiement orange money.

A la fin de la transaction, l'acheteur est redirigé automatiquement vers le site marchand, sur une url définie par le commerçant.

3.2 Appel de la page de paiement

Pour afficher la page de paiement Orange Money, le site web marchand doit envoyer une requête HTTPS de type POST vers l'url du serveur de paiement Orange Money.

La requête doit contenir les variables suivantes:

Variable	Type	Description	Obligatoire
S2M_IDENTIFIANT	10 chiffres	Identifiant du partenaire (fourni par Orange)	O
S2M_SITE	10 chiffres	Identifiant du site marchand (fourni par Orange)	O
S2M_REF_COMMANDE	String	Référence de la commande. Cette valeur doit être unique	O
S2M_COMMANDE	String	Libellé de la commande	O
S2M_DATEH	Date UTC	Date de la transaction au format UTC	O

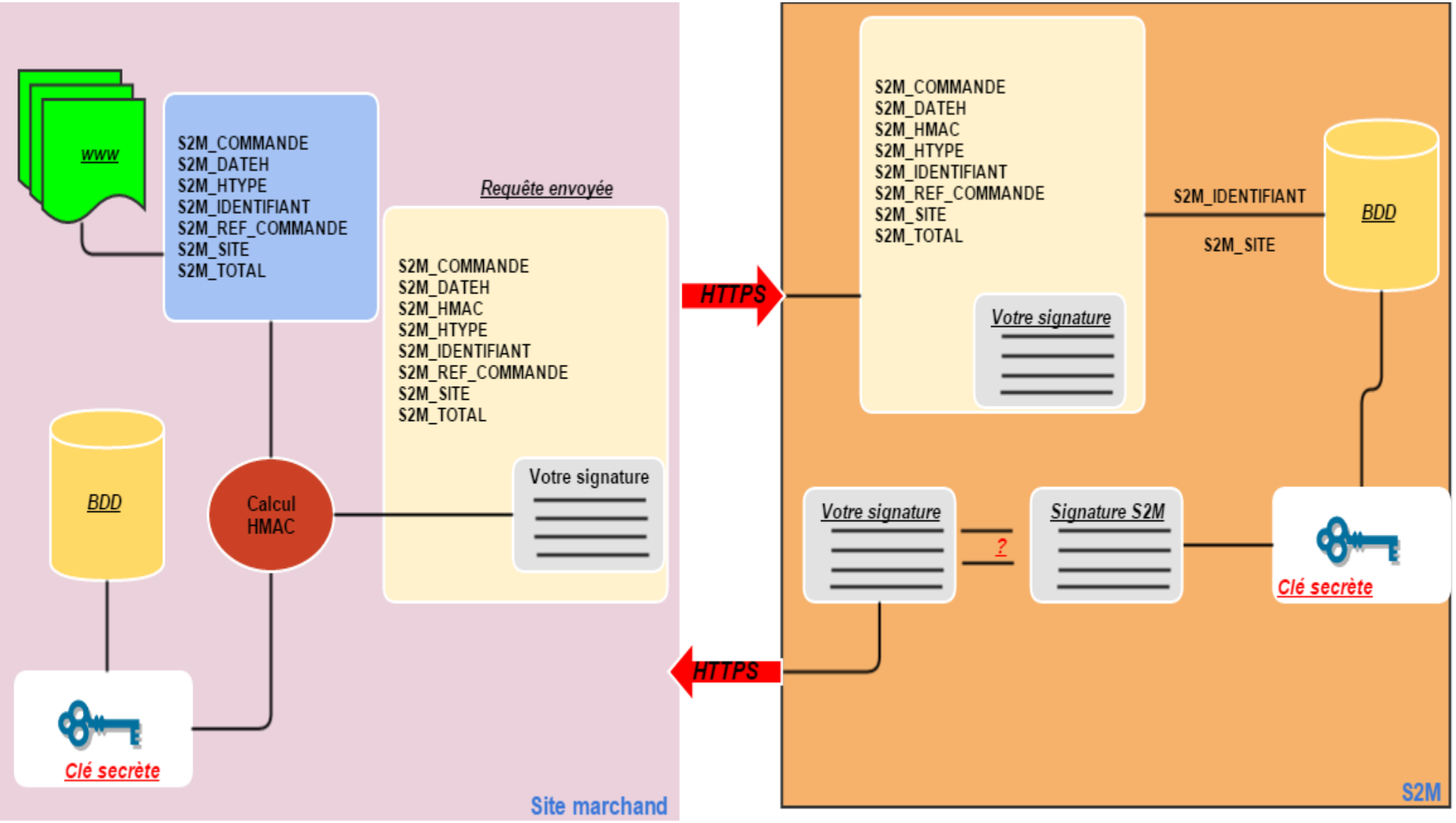
3.2 Appel de la page de paiement

Pour afficher la page de paiement Orange Money, le site web marchand doit envoyer une requête HTTPS de type POST vers l'url du serveur de paiement Orange Money.

La requête doit contenir les variables suivantes:

Variable	Type	Description	Obligatoire
S2M_TOTAL	Float	Total de la commande	O
S2M_HTYPE	String	Algorithme de hashage du message de la transaction	N
S2M_HMAC	String	Hash généré avec la clé secrète du commerçant	O

3.3 Vérification de la requête



3.3 Vérification de la requête (suite)

Une vérification des données envoyées est effectuée, et si la requête est validée, le formulaire de paiement s'affiche.

Le site marchand doit impérativement envoyer son identifiant partenaire et l'identifiant du site marchand dans les variables prévues à cet effet. Pour des raisons de confidentialité, ces valeurs doivent être hashées en md5 et non transmises en clair.

Tous les messages envoyés à la page de paiement doivent être signés par le site marchand via une méthode d'empreinte HMAC de l'ensemble des paramètres transmis.

3.3 Vérification de la requête (suite)

Le processus de signature des messages se fait de la manière suivante:

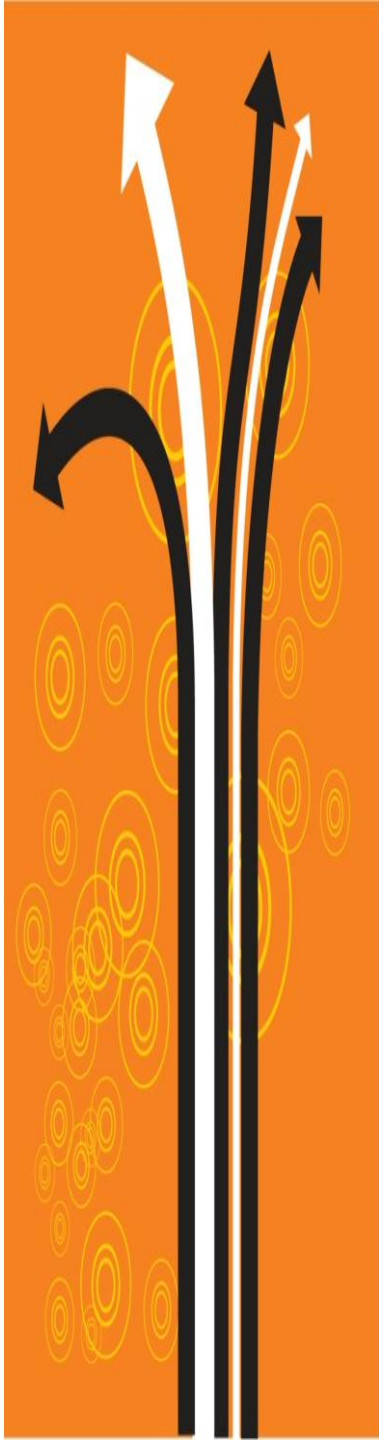
- Former une chaine clé-valeur des variables de la requête séparées par un « & ». (cf. tableau de description des variables plus haut)

  L'ordre des variables est important dans la construction de la chaine: elles doivent suivre un ordre alphabétique naturel.

- Calculer l'empreinte HMAC de la chaine construite précédemment, avec la clé secrète du commerçant et l'algorithme de hashage de son choix.
- Mettre le résultat obtenu dans la variable **S2M_HMAC** de la requête.

  A la réception de la requête, le même procédé est utilisé côté serveur pour valider la demande reçue.

4. Exemple de code



sonatel

orange™

4. Exemple de code PHP

```
<?php

    $dateh = date('c');
    $identifiant = md5('2222222222');
    $ref_commande = OM201503WEBP001';
    $site = md5('1111111111');
    $total = '1250';
    $commande = "TEST Paiement par Orange Money ";
    $algo = "SHA512";
    $cle_secrete =
    "e9e92e5da6ab55c6eb238f2af13a07cc2d9683844bd2
    656dd0e3b1da7f6573f7f329712626a5396b4c11c1946
    4bc05ae8e36cb7da1f5596d237ca64aecf0f458";

    $cle_bin = pack("H*", $cle_secrete);
```

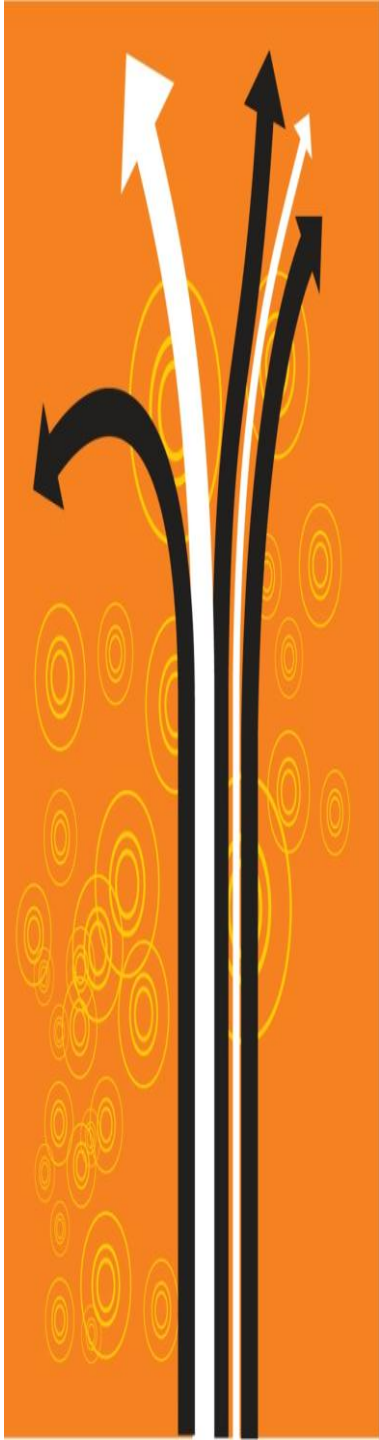
4. Exemple de code PHP (suite)

```
$message =      "S2M_COMMANDE=$commande".
                "&S2M_DATEH=$dateh".
                "&S2M_HTYPE=$algo".
                "&S2M_IDENTIFIANT=$identifiant".
"&S2M_REF_COMMANDE=$ref_commande".
"&S2M_SITE=$site".
"&S2M_TOTAL=$total";

$hmac = strtoupper(hash_hmac(strtolower($algo),
            $message, $cle_bin));

?>
```

4. Exemple de code PHP (suite)

```
<form method="POST" action=« url_gateway">
        <input type="hidden" name="S2M_IDENTIFIANT" value="<?php echo
        $identifiant;?>">
        <input type="hidden" name="S2M_SITE" value="<?php echo $site;?>">
        <input type="hidden" name="S2M_TOTAL" value="<?php echo $total;?>">
        <input type="hidden" name="S2M_REF_COMMANDE" value="<?php echo
        $ref_commande;?>">
        <input type="hidden" name="S2M_COMMANDE" value="<?php echo
        $commande;?>">
        <input type="hidden" name="S2M_DATEH" value="<?php echo $dateh;?>">
        <input type="hidden" name="S2M_HTYPE" value="<?php echo $algo;?>">
        <input type="hidden" name="S2M_HMAC" value="<?php echo $hmac;?>">
        <input type="image" name="submit"      src="http://www.orange-
money.sn/tpl/images/logo.jpg"  style="border: 0px solid black;border-radius: 10px; -moz-
border-radius: 10px; -        khtml-                    border-radius: 10px; -
webkit-border-radius:         10px;"  alt="Payer" />
</form/>
```

5. Gestion des retours



sonatel

orange™

5. Gestion des retours

Une fois le paiement effectué, le client a la possibilité de revenir sur le site commerçant par l'intermédiaire de 3 URLs: une en cas de succès, une en cas d'échec et une en cas d'annulation.

Une 4ème URL permet de gérer les retours transaction, afin de permettre au commerçant de valider les bons de commande.

A la fin de chaque transaction aboutie, un récapitulatif de l'état de la transaction est affichée ainsi qu'un message de redirection automatique vers le site marchand au bout de quelques secondes.

Ces URLs peuvent être être paramétrées par le client à travers le backoffice client.

5. Gestion des retours (suite)

Cette redirection peut se faire vers 3 URLs différentes. Les variables suivantes sont transmises en POST vers chacune de ces 3 URLs:

- ***ref_commande***
- ***montant***
- ***statut***
- ***message***
- ***ref_transaction***
- ***Nota***: Ces trois URLs ne sont pas sécurisées. Elles sont utilisées uniquement pour afficher de l'information à l'acheteur de retour sur le site du commerçant.

5. Gestion des retours (suite)

Si le commerçant souhaite faire un traitement spécifique (validation bon de commande, mise à jour statut commande...etc), il doit se référer à la 4ème URL: l'URL IPN (Instant Payment Notification).

La notification après paiement est faite au travers de l'URL l'IPN.

Cette URL est sécurisée par le système et permet de garantir de manière fiable le retour des informations sur les détails d'une transaction.

5. Gestion des retours (suite)

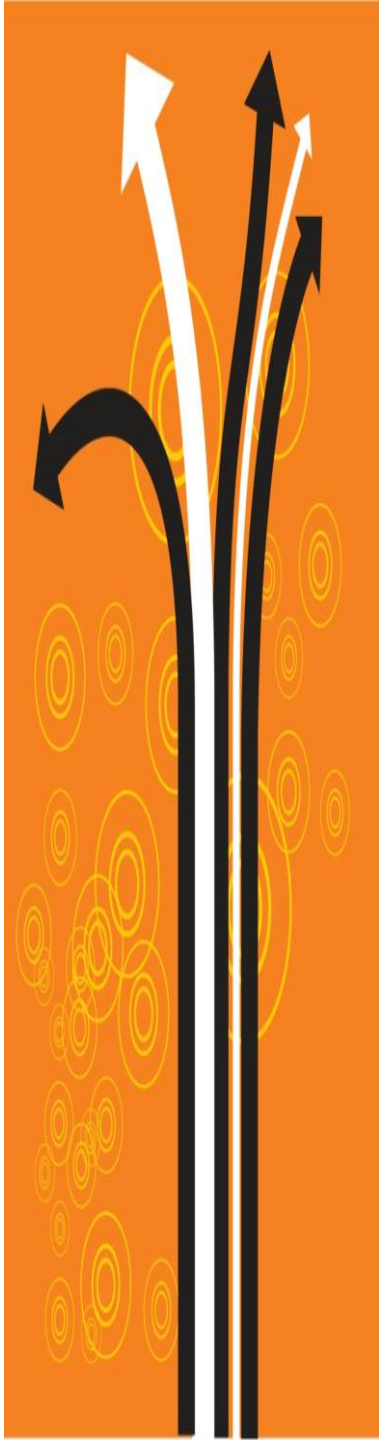
Les informations de la transaction sont transmises à travers les variables suivantes vers l'URL IPN en POST:

- ***- ALGO***
  - CMD
  - HMAC
  - ID
  - MONTANT
  - REF_CMD
  - STATUT
  - TRX_ID
  - UID
- ***PS: A la réception des données, le marchand doit vérifier l'authenticité de celles-ci à travers le même mécanisme que pour l'appel de la page de paiement en générant une empreinte HMAC à l'aide de sa clé secrète et comparer cette empreinte à la valeur de la variable « HMAC » reçue.***

4. Exemple de code PHP

```
<?php

    $_POST = array(
                'ALGO'                          => 'SHA256',
                'CMD'                           => 'Sample transaction',
                'HMAC'                          => 'EC158B8193FFF7E01C768FE320DDBE234234C9D0',
                'ID'                            => '2570239429.1012158196.92347',
                'MONTANT'       => '8500',
                'REF_CMD'       => 'SAMPLE_REF_CMD',
                'STATUT'        => '200',
                'TRX_ID'        => 'MP173453.3454.A12687',
                'UID'                           => '5894f79a37e6d'
                                                );
    $data = $_POST;
    $secret_key = '05E964F202FD9D53DC51F2760C03661JDL93SD0DCCD1A94055639D8545E53D63';
    $bin_key = pack("H*", $secret_key);
    ksort($data);
    $message = urldecode(http_build_query($data));
    $hmac = strtoupper(hash_hmac(strtolower($data['ALGO']), $message, $bin_key));
    if ($hmac === $_POST['HMAC'])
                echo 'Bingo! Valid Data';
                // Process data
    else
                die('Suspicious data!');
```

6. Codes de retour



sonatel

orange™

6. Codes de retour

Code	Description
117	Transaction failed
200	Transaction successeful
220	Transaction not found
375	OTP is expired or already used or invalid

Merci

sonatel

orange™