



Module CMI

Intégration du paiement en ligne des sites Marchands

Version 1.4.4

Historique des versions

N° de version	Date de version	Nature de la modification
V1.0	05 Novembre 2015	Création
V1.1	19 November 2016	Le paramètre « encoding » avec la valeur « utf-8 »
V1.2	02 February 2017	Le paramètre « shopurl »
V1.3	02 March 2017	Les paramètres « currenciesList », « amountCur » et « symbolCur »
V1.3.1	13 Avril 2017	BUSINESSDATE
V1.3.2	18 Août 2017	Le paramètre %autoRedirect+
V1.4	06 Août 2018	Table des codes erreurs + Etats des transactions + Contrôle et suivi des Callbacks
V1.4.1	12 Décembre 2018	Correction de la casse du paramètre %AutoRedirect+
V1.4.2	14 Février 2019	<ul style="list-style-type: none"> • Format du paramètre « BillToCountry » • Les paramètres « BillToName » et « email » sont obligatoires • Nouveau paramètre « sessiontimeout » • Calcul du code de hachage dans le cas d'articles contenant le mot « document » • Ajout du code erreur ISO8583-13
V1.4.3	13 Mai 2019	Nouvelle réponse marchand « FAILURE » au callback CMI
V1.4.4	14 Janvier 2020	<ul style="list-style-type: none"> • Taille du paramètre « description » modifiée. • Mise à jour de la liste des codes erreurs. • Remarque par rapport au calcul de hash.

Sommaire

1. INTRODUCTION	3
2. SECURITE DES ECHANGES.....	3
3. PROCESSUS DE PAIEMENT EN LIGNE PAR CARTE BANCAIRE	4
3.1. Etapes :	4
3.1.1. Diagramme de flux :	6
4. DONNEES ECHANGEES.....	7
4.1. REQUETE DE DEMANDE DE PAIEMENT :	7
4.1.1. Paramètres :	7
4.1.2. Exemple de requête de paiement:.....	11
4.1.3. Génération du code de hachage de la requête de paiement :	12
4.2. RÉSULTAT DE PAIEMENT :	13
4.2.1. La requête de callback host-to-host:	13
4.2.2. Redirection vers le site marchand:.....	15
4.2.3. Paramètres de la requête du résultat de paiement:.....	16
4.2.4. Génération de la clé du hachage du résultat de paiement:.....	18
4.2.5. Exemple de données de la requête du résultat de paiement.....	18
4.2.6. Suivi des callbacks via le Merchant Center CMI.....	20
5. ETATS DES TRANSACTIONS.....	22
5.1. PRE AUTORISATION :	22
5.2. POST AUTORISATION :	22
5.3. REMBOURSEMENT :	23
5.4. ANNULATION :	24
6. ANNEXE.....	26
6.1. Contact du service Intégration ECOM du CMI:	26
6.2. Codes d'erreurs :	26

1. INTRODUCTION

Ce document a pour objectif de décrire en détail les spécifications techniques pour interfacer un site marchand avec la plate-forme de paiement en ligne du Centre Monétique Interbancaire (CMI).

2. SECURITE DES ECHANGES

Pour la sécurisation des transactions de paiement en ligne, le CMI utilise en standard le protocole SSL pour le chiffrement des informations de commande du site marchand, des coordonnées bancaires du client et des écrans de gestion des transactions destinés aux marchands. Pour cela, le CMI est doté de certificats de sécurité SSL signés par des autorités de certification reconnues.

La sécurité est assurée à plusieurs niveaux.

- Sur le site marchand, chaque requête de paiement en ligne est accompagnée par un code de hachage généré par un algorithme de hachage et une clé secrète. Cette clé est générée par le marchand et configurée sur son espace d'administration de la plate-forme de paiement.
- Sur la plate-forme, le même algorithme de hachage est utilisé avec la clé secrète partagée du marchand pour authentifier le site marchand et vérifier qu'aucun élément de la requête de paiement n'ait été modifié pendant son transfert sur le réseau.
- La saisie des informations nécessaires aux traitements financiers est sécurisée par le protocole SSL avec d'autres algorithmes non décrits dans ce document.

Les fonctions de cryptographie ne sont pas accessibles à l'utilisateur et à fortiori ne peuvent pas être modifiées ou complétées.

3. PROCESSUS DE PAIEMENT EN LIGNE PAR CARTE BANCAIRE

3.1. Etapes :

Le processus de paiement en ligne par cartes bancaires se déroule selon les étapes suivantes :

- Le client génère sa commande dans le site marchand et choisi de payer en ligne par cartes bancaires.
- Le client est redirigé vers la plate-forme CMI qui affiche la page de paiement. Sur cette page est affiché un récapitulatif de la demande de paiement dont le montant de la transaction. Le client est ainsi invité à saisir ses coordonnées bancaires (le n° de sa carte de paiement, sa date d'expiration et son code CVS).
- Lorsque le client valide sa demande, la plate-forme de paiement vérifie si la carte est authentifiable. Le cas échéant, une page d'authentification forte est affichée au client où il est censé saisir son code secret d'authentification qui est vérifié par sa banque.
- Si l'authentification forte du client réussit, la plate-forme de paiement envoie une demande d'autorisation à l'acquéreur (CMI) qui la traite avec la banque émettrice.
- Si l'autorisation de paiement est refusée (fonds insuffisants, dépassement du plafond autorisé sur la carte, carte blacklistée, etc.), un message d'erreur est affiché à l'écran du client. Dans ce cas, le client peut faire une autre tentative en saisissant ses coordonnées bancaires une deuxième fois.

Remarque : Le message d'erreur affiché au client ne donne pas forcément la raison exacte du rejet. Ceci est conforme aux normes de prévention de fraude. Si le client a besoin de connaître la raison de l'échec de paiement, il est censé prendre contact avec sa banque. Le marchand, quant à lui, a accès au message de retour de la Banque et ce via son espace CMI de suivi des transactions en ligne.

- Si l'autorisation est accordée par la banque du client,
 - Si le site marchand a demandé dans la demande initiale de paiement, une requête de confirmation de paiement est envoyée automatiquement et en background (server-to-server) de la plate-forme CMI vers le site marchand.
 - A la réception de la requête de confirmation de paiement, le site marchand identifie la commande dans sa base de données et procède à la mise à jour de son état et l'enregistrement des informations de paiement contenues dans la requête. Il retourne aussi une réponse à la plate-forme CMI pour confirmer la bonne prise en compte du paiement. Ce retour peut aussi servir à demander de confirmer la transaction pour débiter le client ou d'annuler la transaction pour lever le blocage de l'acceptation de l'autorisation de paiement.
 - Au niveau de la plate-forme CMI, un reçu en ligne est affiché au client reprenant les informations de la commande et du paiement (Identifiant de la commande, N° de paiement, date de paiement, méthode de paiement, etc.). Ce reçu peut contenir un lien qui permet au client de retourner au site marchand et compléter le processus de commande.

Remarque : Quand la banque du client accepte une autorisation de paiement (la demande de paiement initiale), elle procède au blocage du montant de la transaction dans le compte du client. Il s'agit d'un blocage de garantie de paiement qui dure en moyenne 7 jours. Ce blocage est levé :

- Soit lorsque la transaction est confirmée (et le compte client est débité),
- Soit lorsque le marchand annule une transaction le jour même de son autorisation.
- Soit si aucun ordre de remise ne parvient à la banque dans le délai de garantie de paiement (7 jours).

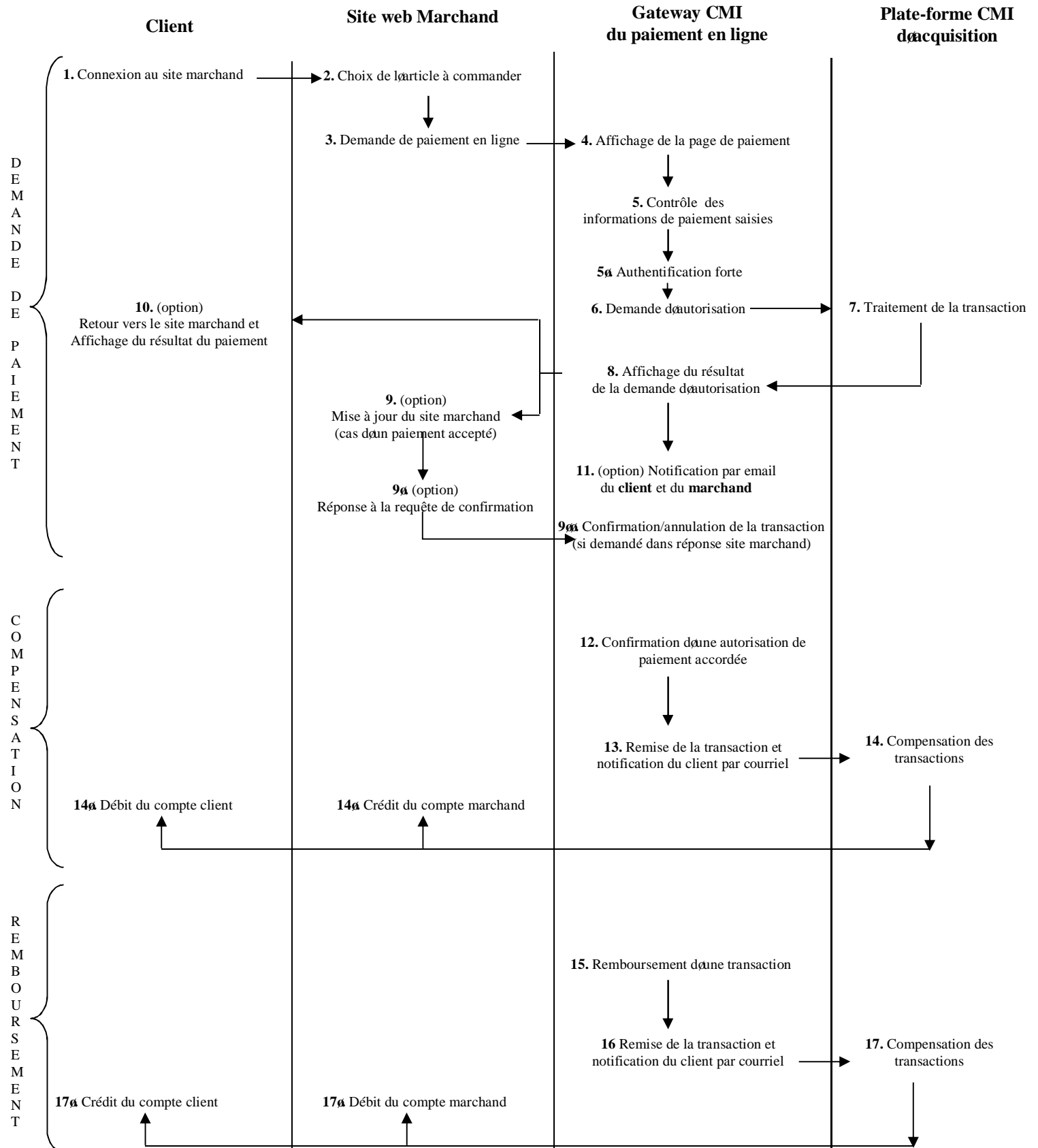
- Dans le cas de transaction confirmée (manuellement via le back office de la plate-forme ou automatiquement via la requête de confirmation de paiement en mode server-to-server ou via les APIs), la remise de la transaction est acheminée par la plate-forme CMI à l'acquéreur qui traite la compensation des comptes (débit du compte client et crédit du compte marchand).

Remarque : Le compte du marchand est crédité du montant total des transactions télécollectées dans la journée par le CMI. Les frais de traitement du CMI, étant prélevés à la source, sont déduits du montant total.

- Le marchand a la possibilité de rembourser en ligne son client via le back office de la plate-forme de paiement ou via les APIs.
- Des notifications sont envoyées par la plate-forme CMI sous forme de courriels aussi bien aux clients qu'aux marchands.

Remarque : Les notifications de la plate-forme CMI sont activées par défaut mais peuvent être désactivées suite à la demande du marchand.

3.1.1. Diagramme de flux :



4. DONNEES ECHANGEES

L'échange de données entre le site marchand et la plate-forme CMI se fait à travers un envoi de formulaire HTTP (form Post). Cet envoi est sécurisé en signant chaque échange avec un algorithme de hachage et une clé secrète.

4.1. REQUETE DE DEMANDE DE PAIEMENT :

Formulaire de demande de paiement envoyé par le site marchand vers la plate-forme CMI lors de la redirection du client pour le paiement en ligne.

4.1.1. Paramètres :

Cette section fournit une description des attributs nécessaires pour la création de la demande de paiement. Ces attributs, sont en général organisés selon les catégories suivantes :

- Attributs obligatoires
- Attributs optionnels

Attributs obligatoires

Nom de l'attribut	Description	Format	Contrainte
clientid	Identifiant du marchand (attribué par le CMI)	Alphanumérique (15)	Requis
storetype	Modèle du paiement du marchand	Alphanumérique (15)	Requis Valeur à utiliser pour la page de paiement web : « 3d_pay_hosting »
trantype	Type de la transaction	Alphanumérique (15)	Utiliser la valeur %ReAuth+pour la pré autorisation
amount	Montant de la transaction	Numérique Valeur du montant sans symbole monétaire. Utiliser « . » ou « , » pour le séparateur du décimal. Exemple : 29.95	Requis
currency	Code ISO de la devise de la transaction	Numérique (3)	Requis Le code numérique ISO 4217 de la devise. Code ISO du MAD : 504

oid	Identifiant de la commande/caddie dans la BDD du site marchand	Alphanumérique (64)	Requis
okUrl	L'URL utilisée pour rediriger le client vers le site marchand en cas d'autorisation de paiement acceptée.	URL	Requis
failUrl	L'URL utilisée pour rediriger le client vers le site marchand en cas d'autorisation de paiement échouée.	URL	Requis
lang	La langue utilisée lors de l'affichage des pages de paiement.	Alphabétique (2)	Requis Valeurs possibles : • ar: Arabe • fr: Français • en: Anglais Par défaut « fr »
email	Adresse électronique du client	Alphanumérique (64)	Requis Format email
BillToName	Nom (et prénom) du client	Alphabétique (255)	Requis
rnd	Chaîne de caractères aléatoire utilisée dans le code de hachage	Alphabétique (20)	Requis
hash	Code hachage de contrôle	Alphanumérique	Requis (Voir plus bas la méthode de génération du code de hachage)
hashAlgorithm	Version du hachage	Alphanumérique	Requis Valeur à utiliser : %r3+

• **Attributs optionnels**

Nom de l'attribut	Description	Format	Contrainte
encoding	Encodage des données de la requête de paiement	Alphanumeric (32)	Optionnel Valeur à utiliser : %utf-8+
description	Description envoyée à l'API	Alphanumeric (125)	Optionnel
tel	N° de téléphone du client	Alphanumérique (32)	Optionnel

BillToStreet1	Adresse 1 du client	Alphanumérique (255)	Optionnel
BillToStreet2	Adresse 2 du client	Alphanumérique (255)	Optionnel
BillToCity	Ville du client	Alphanumérique (64)	Optionnel
BillToStateProv	Etat/Province du client	Alphanumérique (32)	Optionnel
BillToPostalCode	Code postal du client	Alphanumérique (32)	Optionnel
BillToCountry	Code du pays du client.	Alphanumérique (3)	Optionnel
idN	Identifiant de l'article #N. Requis pour l'article #N.	Alphanumérique (128)	Optionnel Quand il y a un seul article, N prend la valeur 1. Dans ce cas, le nom du paramètre devient : id1.
itemnumberN	Numéro de l'article #N	Alphanumérique (128)	Optionnel
productcodeN	Code-produit de l'article #N	Alphanumérique (64)	Optionnel
qtyN	Quantité de l'article #N	Numerique	Optionnel
descN	Description de l'article #N	Alphanumérique (128)	Optionnel
priceN	Prix unitaire de l'article #N	Numérique Valeur du montant sans symbole monétaire. Utiliser « . » ou « , » pour le séparateur du décimal. Exemple : 29.95	Optionnel
totalN	Sous-total de l'article #N	Numérique Valeur du montant sans symbole monétaire. Utiliser « . » ou « , » pour le séparateur du décimal. Exemple : 29.95	Optionnel
CallbackResponse	Activer/Désactiver la requête de confirmation de paiement en mode server-to-server	Booléen	Optionnel Valeurs possibles : • true: Activé • false: Désactivé Par défaut « true »
CallbackURL	L'URL utilisée dans la requête de confirmation de paiement en mode server-to-server	URL	Optionnel
shopurl	L'URL de retour vers laquelle le client est redirigé lorsqu'il clique sur le bouton "Annuler" affiché sur la page de paiement.	URL	Optionnel
currenciesList	Utilisé pour afficher (ou non) la liste des devises de change dans les pages de paiement. Cette liste est	Boolean	Optionnel Valeurs possibles :

	générée par la plateforme CMI ECOM. Dans ce cas, le marchand ne gère pas les valeurs listées. Si le commerçant souhaite afficher, sur la page de paiement, une valeur de change calculée par son site web, il devra utiliser les paramètres "amountCur" et "symbolCur".		<ul style="list-style-type: none"> • true: Activé • false: Désactivé Par défaut « false »
amountCur	La conversion du montant dans une devise étrangère, à montrer au client dans la page de paiement. Dans ce cas, la valeur du montant de conversion est calculée par le site marchand (contrairement au cas où le paramètre "currenciesList" est utilisé).	Numérique Amount value without currency symbol. Use "." or "," as decimal separator. Example: 29.95	Optionnel
symbolCur	Symbole de la devise de conversion à afficher dans la page de paiement avec la valeur du paramètre "amountCur"	Alphanumérique	Optionnel Exemples : EUR, USD.
AutoRedirect	Utilisé pour rediriger le client automatiquement vers le site marchand lorsque la transaction de paiement en ligne est traitée.	Boolean	Optionnel Valeurs possibles : <ul style="list-style-type: none"> • true: Activé • false: Désactivé Par défaut « false »
sessiontimeout	Permet de définir le délai d'expiration de la session de la page de paiement.	Numérique Le paramètre est calculé en secondes.	Optionnel Exemple : 600 (pour une session de 10 minutes) Par défaut: 1800 secondes. La valeur minimale autorisée est 30 secondes et la valeur maximale est 2700 secondes.

Remarques :

- Il est recommandé que la mise à jour de l'état de paiement de la commande dans le site marchand soit faite via la confirmation server-to-server utilisant le paramètre CallbackURL. Les paramètres okUrl et failUrl peuvent être utilisés pour ce faire, mais ils requièrent la redirection (html) des clients vers le site marchand.
- L'URL renseignée dans le paramètre CallbackURL doit être accessible sur Internet même lors de la phase de test.
- L'URL renseignée dans le paramètre CallbackURL ne doit pas nécessiter une authentification d'accès (login/password). Cela dit, il se peut que l'équipe Intégration ECOM du CMI exige ces données lors des tests d'intégration.
- Il est fortement recommandé d'utiliser le paramètre « encoding », même s'il est optionnel, et ce pour éviter des problèmes lorsque les données contiennent des caractères spéciaux.
- Il faut veiller à respecter la taille de chaque paramètre de la requête de demande de paiement.

4.1.2.Exemple de requête de paiement:

```
<form method="post" action="https://host/fim/est3dgate ">
  <input type="hidden" name="clientid" value="990000000000001"/>
  <input type="hidden" name="storetype" value="3d_pay_hosting" />
  <input type="hidden" name="hash" value="iej6cPOjDd4IKqXWQEznXWqLzLI=" />
  <input type="hidden" name="trantype" value="PreAuth" />
  <input type="hidden" name="amount" value="31.50" />
  <input type="hidden" name="currency" value="504" />
  <input type="hidden" name="oid" value="1291899411421" />
  <input type="hidden" name="okUrl" value="https://www.teststore.ma/success.php" />
  <input type="hidden" name="failUrl" value="https://www.teststore.ma/fail.php" />
  <input type="hidden" name="lang" value="fr" />
  <input type="hidden" name="rnd" value="asdf" />
  <input type="hidden" name="hashAlgorithm" value="ver3">

Optional parameters
  <input type="hidden" name="tel" value="012345678">
  <input type="hidden" name="email" value="test@test.ma">

<!-- Billing Parameters [All Optional]-->
  <input type="hidden" name="BillToCompany" value="Billing Company">
  <input type="hidden" name="BillToName" value="Bill John Doe">
  <input type="hidden" name="BillToStreet1" value="Address line 1">
  <input type="hidden" name="BillToStreet2" value="Address line 2">
  <input type="hidden" name="BillToCity" value="Casablanca">
  <input type="hidden" name="BillToStateProv" value=" Casablanca">
  <input type="hidden" name="BillToPostalCode" value="12345">
  <input type="hidden" name="BillToCountry" value="504">

<!-- Order Item Parameters [All Optional]-->
  <input type="hidden" name="ItemNumber1" value="a5">
  <input type="hidden" name="ProductCode1" value="a5">
  <input type="hidden" name="Qty1" value="3">
  <input type="hidden" name="Desc1" value="a5 desc">
  <input type="hidden" name="Id1" value="a5">
  <input type="hidden" name="Price1" value="10.50">
  <input type="hidden" name="Total1" value="31.50">

</form>
```

4.1.3. Génération du code de hachage de la requête de paiement :

L'approche de hachage est utilisée pour authentifier les utilisateurs lors des demandes de paiement. Pour générer le code de hachage, ajoutez toutes les valeurs des paramètres de la requête de paiement postés dans l'ordre alphabétique (A à Z) en utilisant le pipeline "|" comme séparateur entre les paramètres. Si un paramètre est envoyé à la plate-forme CMI avec une valeur vide, il sera toujours ajouté aux données de hachage (pour un exemple de valeur vide, voir dans l'exemple ci-dessous la valeur du paramètre « email »).

Après que tous les paramètres de la requête soient ajoutés alphabétiquement en utilisant le pipeline "|" comme séparateur, le paramètre storeKey est ajouté à la fin des données de hachage en utilisant aussi le pipeline "|".

Notez que dans le cas d'utilisation du caractère "|" dans la valeur de l'un des paramètres de la requête, le caractère "\" est utilisé pour l'échappement. Par conséquent, si le caractère "\" est également utilisé dans la valeur d'un paramètre, il faut utiliser le caractère "\" avant, puis l'ajouter au hachage du texte brut. Pour une meilleure compréhension, vous pouvez vérifier l'exemple ci-dessous:

Original Value	: ORDER-256712jbs\j6b
Value used for Hash Calculation	: ORDER-256712jbs\\j6b\\

Exemple de paramètres et calcul du code de hachage :

clientId	100200127
amount	95.93
okurl	http://localhost:8080/SampleCodeJSPTTest/GenericVer3ResponseHandler
failUrl	http://localhost:8080/SampleCodeJSPTTest/GenericVer3ResponseHandler
TranType	PreAuth
email	
callbackUrl	http://localhost:8080/SampleCodeJSPTTest/GateResponseControl.jsp
currency	504
rnd	87954458746
storeType	3d_pay_hosting
lang	en
hashAlgorithm	ver3
BillToName	name
BillTocompany	billToCompany
storeKey	ABCD1234

Code de hachage :

Order of Used Parameters in Hash Data :

amount|BillToCompany|BillToName|callbackUrl|clientid|currency|email|failUrl|hashAlgorithm|language|okurl|rnd|storetype|TranType|storeKey

Plaintext:

95.93|billToCompany|name|http://localhost:8080/SampleCodeJSPTTest/GateResponseControl.jsp|100200127|504||http://localhost:8080/SampleCodeJSPTTest/GenericVer3ResponseHandler|ver3|en|http://localhost:8080/SampleCodeJSPTTest/GenericVer3ResponseHandler|87954458746|3d_pay_hosting|PreAuth|ABCD1234

Hash = Base64(SHA512(plaintext))

Remarque:

- Les paramètres "encoding" et "hash" sont ignorés pendant le calcul du hachage.
- Pour des raisons de sécurité, la plateforme CMI utilise un outil qui permet de détecter, prévenir et désactiver l'exécution de scripts non-autorisés (code contenu dans les paramètres HTTP). Donc il faut remplacer tout caractère après la chaîne « document » par un point "." au moment du calcul du hachage.
Exemples :
document abc -> document.abc
documentabc -> document.bc
- Afin d'éviter une erreur de hachage, il faut s'assurer que les valeurs des paramètres calculées sont les mêmes que celles envoyées dans la requête de demande de paiement.
Par exemple l'ajout d'un bouton de soumission qui effectuera l'action d'envoyer le formulaire de demande de paiement risque d'influencer le calcul de hash. Pour remédier à cela, il faut prendre en compte la valeur de cet élément (bouton) dans le calcul de hash ou bien supprimer son attribut « name ».

4.2. RÉSULTAT DE PAIEMENT :

Lorsque le client valide la page de paiement avec les données de la carte, le flux d'authentification 3D commence. Une fois le processus d'authentification 3D terminé, l'autorisation de paiement est traitée avec la banque émettrice du client. Les paramètres de réponse de paiement ainsi que tous les paramètres envoyés par le marchand dans la demande de paiement seront retournés au marchand pour confirmer le paiement et mettre à jour le statut de la commande dans sa base de données.

4.2.1. La requête de callback host-to-host:

Le marchand démarre le flux de paiement en envoyant le client vers la plateforme du CMI pour demander une autorisation de paiement (PreAuth). Dans cette requête, le paramètre CallbackResponse doit prendre la valeur « true » et le paramètre CallbackUrl doit être renseigné afin que la plateforme CMI puisse envoyer une requête de callback au site marchand après traitement de la transaction. A la réception de la requête de callback du CMI, le site marchand est censé retourner une réponse afin de décider du débit ou non du client.

Réponse du site web marchand :

Les réponses du callback suivantes sont possibles :

- **Accusé de réception** : la réponse du site marchand dans ce cas est comme suit : APPROVED. La transaction est reconnue par le marchand mais il demande de ne pas débiter le client. Le marchand doit confirmer ou annuler manuellement la transaction via son back office CMI.
- **Demande de débit du client** : la réponse du site marchand dans ce cas est comme suit : ACTION=POSTAUTH. Dans ce cas, une demande de confirmation automatique de la transaction (PostAuth) sera envoyée à la banque émettrice pour débiter le compte client du montant de la transaction.
- **Echec** : la réponse du site marchand dans ce cas est comme suit : FAILURE. La transaction n'a pas pu être prise en compte par le site marchand. Le client est invité à vérifier le statut de sa commande sur le site du marchand. Le marchand doit confirmer ou annuler manuellement la transaction via son back office CMI.
- **Timeout** : Si aucune réponse ne parvient à la plate-forme CMI de la part du site web du marchand, le client est invité à vérifier l'état de sa commande en retournant vers le site du marchand. Dans ce cas, le marchand doit traiter manuellement la transaction via son back office CMI selon l'état de la commande dans sa BDD.
- **Erreur de syntaxe** : S'il y a une erreur dans la réponse du site marchand, le client est invité à vérifier l'état de sa commande en retournant au site marchand. Dans ce cas, le marchand doit traiter manuellement la transaction via son back office CMI selon l'état de la commande dans sa BDD.

Contrôles du site web marchand :

Voici les actions que le site web marchand est censé entreprendre lors de la requête du callback de la plate-forme CMI :

- Générer un hash avec les mêmes données postées par le CMI dans le callback, puis comparer le hash calculé avec le hash envoyé par le CMI. S'ils sont identiques, passer à la vérification suivante.
- Chercher, dans la BDD des commandes du site web marchand, l'enregistrement identifié par la valeur du paramètre « oid » qui est envoyé par le CMI dans la requête du callback.
- Vérifier si le montant de la commande enregistré dans la BDD des commandes du site web marchand est égal au montant envoyé par le CMI dans la requête du callback via le paramètre « amount ».

- Vérifier la valeur du paramètre « ProcReturnCode » envoyé par le CMI dans la requête du callback :
 - Si ProcReturnCode = 00, il s'agit d'une transaction acceptée.
 - Donc il faut mettre à jour l'état de la commande dans la BDD des commandes du site web marchand (état = Payée).
 - Répondre à la requête du callback du CMI par :
 - « ACTION=POSTAUTH » : pour que le client soit débité automatiquement.
 - « APPROVED » : pour que le client ne soit pas débité automatiquement. Dans ce cas, le marchand doit confirmer ou annuler manuellement la transaction via son back office CMI.
 - Si ProcReturnCode <> 00 ou si le paramètre ProcReturnCode n'existe pas dans la requête du callback du CMI, il s'agit d'un échec d'autorisation de paiement.
 - Dans ce cas, il ne faut pas modifier l'état de la commande dans la BDD des commandes du site web marchand.
 - La réponse à retourner à la requête du callback du CMI est « APPROVED » (pour accusé de réception).
 - Si un problème technique a lieu lors l'une des étapes précédentes, répondre à la requête du callback du CMI par « FAILURE ». Dans ce cas, le marchand doit confirmer ou annuler manuellement la transaction via son back office CMI.

Remarque:

- Ce qu'il faut noter aussi pour cette requête de callback en mode server-to-server, c'est qu'elle envoie au site web marchand aussi bien des cas de transactions réussies que des cas de rejets. Donc il se peut très bien que le site marchand reçoive, pour la même commande, des retours d'échecs qui seront suivis par un retour d'acceptation de transaction. Cela signifie que le client a procédé à des tentatives échouées avant qu'il réussisse sa dernière tentative. C'est le paramètre ProcReturnCode qui permet de faire la distinction entre les requêtes du callback des autorisations de paiement réussies (ProcReturnCode = 00) et les requêtes du callback des échecs de paiement (ProcReturnCode != 00 ou inexistant).

4.2.2. Redirection vers le site marchand:

Lorsqu'une transaction est traitée, un lien est affiché dans la page du résultat de paiement afin que le client puisse retourner vers le site Web du marchand.

Dans le cas d'une transaction approuvée, le client sera redirigé vers okUrl (paramètre envoyé par le site marchand dans la demande de paiement). Toutes les données reçues dans la demande de paiement du site marchand, ainsi que toutes les données de la transaction traitée seront envoyées par la plateforme CMI vers okUrl. Dans ce cas, la valeur du paramètre "Response" (voir détail de ce paramètre plus loin) sera "Approved".

Dans le cas d'une transaction échouée, le client sera redirigé vers failUrl (paramètre envoyé par le site marchand dans la demande de paiement). Toutes les données reçues dans la demande de paiement

du site marchand, ainsi que toutes les données de la transaction traitée seront envoyées par la plate-forme CMI vers failUrl. Dans ce cas, la valeur du paramètre "Response" sera "Declined" ou "Error".

Remarque:

- En général, la mise à jour de l'état de paiement de la commande au niveau du site marchand se fait au moment de la requête du callback server-to-server (via la CallbackURL). Il est recommandé que le site marchand vérifie aussi l'état de paiement de la commande au moment de la redirection du client vers la okURL ou la failURL. En effet, dans le cas où la requête du callback server-to-server (via la CallbackURL) échoue, la redirection du client vers la okURL ou la failURL peut être utilisée pour prendre en compte l'état de paiement effectué au niveau de la plate-forme du CMI. Il faut juste se rappeler que dans le cas de la requête du callback server-to-server (via la CallbackURL), la plate-forme CMI s'attend à une réponse du site marchand pour décider si le client doit être débité ou non ; tandis que dans le cas de la redirection du client vers la okURL ou la failURL, aucune réponse n'est attendue à partir du site marchand. Donc dans ce cas le marchand doit traiter manuellement la confirmation de la transaction via son Merchant Center CMI pour débiter le client le cas échéant.

4.2.3. Paramètres de la requête du résultat de paiement:

Lorsque la plate-forme CMI renvoie le résultat du paiement au site marchand (soit via la requête callback host-to-host, ou soit via la redirection http du client), la requête contient, en plus des paramètres envoyés par le site marchand dans la demande de paiement, les paramètres suivants qui concernent le traitement de la transaction :

Nom de l'attribut	Description	Format	Contrainte
Response	Etat de paiement	Alphabétique	Valeurs possibles : "Approved", "Error", "Declined"
ProcReturnCode	Code d'état de la transaction	Alphanumérique (2)	Valeurs possibles : %00+pour les transactions autorisées, %09+pour les rejets de la plate-forme, autres pour les codes d'erreur ISO-8583
EXTRA.TRXDAT E	Date de la transaction	Alphanumérique (17)	Format : "jj/mm/0aaaa hh24:mi:ss"
AuthCode	Code d'autorisation de la banque	Alphanumérique (6)	
acqStan	Identifiant de paiement de l'acquéreur	Numérique (6)	
HostRefNum	Numéro de référence de la transaction	Alphanumérique (12)	
TransId	Identifiant de la transaction dans la plateforme CMI	Alphanumérique (64)	
ErrMsg	Message d'erreur	Alphabétique (255)	
ClientIp	Adresse IP du client	Alphanumérique (15)	Format comme : "###.###.###.###"
ReturnOid	Identifiant de la commande du site marchand	Alphanumérique (64)	Doit être identique à l'input OID (envoyé dans la requête de paiement du marchand)
paymentType	Méthode de paiement utilisée	Alphanumérique	Valeurs possibles : CARD
EXTRA.CARDBR AND	Nom de marque de la carte	Alphabétique	Valeurs possibles : VISA, MASTERCARD, CMI

MaskedPan	Numéro masqué de la carte de paiement	Alphanumérique (19)	Format : XXXXXX*****XXXX
cardHolderName	Nom du porteur de la carte de paiement renseigné par le client au moment du paiement en ligne	Alphanumérique	
Ecom_Payment_Card_ExpDate_Year	Année d'expiration de la carte	Numérique (2)	
Ecom_Payment_Card_ExpDate_Month	Mois d'expiration de la carte	Numérique (2)	
EXTRA.CARDISSUER	Nom de l'émetteur de la carte	Alphabétique	
merchantID	Identifiant CMI du marchand	Alphanumérique (15)	
ACQBIN	Identifiant du acquéreur	Numérique (6)	
mdStatus	Etat de l'authentification en ligne du porteur	Numérique (1)	Valeurs possibles : 1= transaction authentifiée (Full 3D) 2, 3, 4 = Carte ne participant pas ou tentative (Half 3D) 5,6,7,8 = Authentification non disponible ou erreur système 0 = Authentification échouée
txstatus	Etat de l'authentification en ligne du porteur	Alphabétique (1)	Possible values "A", "N", "Y"
iReqCode	Code fourni par l'ACS lorsque le traitement ne peut pas être effectué pour une raison quelconque.	Numérique (2)	
iReqDetail	Détail concernant le paramètre iReqCode.	Alphanumérique	
vendorCode	Message d'erreur décrivant l'erreur iReqDetail.	Alphanumérique	
PAResSyntaxOK	Information à propos du résultat d'authentification en ligne du porteur.	Alphabétique (1)	Valeurs possibles "N", "Y"
ParesVerified	Information à propos de la signature d'authentification en ligne du porteur.	Alphabétique (1)	Valeurs possibles "N", "Y"
eci	Indicateur d'authentification en ligne du porteur.	Numérique (2)	
cavv	Valeur de vérification de l'authentification du porteur.	Alphanumérique (28)	
xid	Identifiant unique de transaction en ligne	Alphanumérique (28)	Encodé en Base64
cavvAlgorithm	Algorithme CAVV	Numérique (1)	Possible values "0", "1", "2", "3"
md	Données MPI identifiant l'authentification en ligne du porteur	Alphanumérique	
Version	Informations sur la version MPI	Alphanumérique (3)	
sID	ID de schéma	Numérique (1)	
MdErrorMsg	Message d'erreur de MPI (le cas échéant)	Alphanumérique (512)	
HASH	Valeur de la clé du hachage	Alphanumérique (20)	

4.2.4. Génération de la clé du hachage du résultat de paiement:

(Utilisez la même technique que la génération de la clé du hachage de la demande de paiement - Voir ci-dessus)

4.2.5. Exemple de données de la requête du résultat de paiement

Cas de transaction réussie :

Parameter	Value	Parameter	Value
ACQBIN	439218	INVOICENUMBER	
acqStan	56928	iReqCode	
amount	27.47	iReqDetail	
AuthCode	746579	itemnumber1	a1
Bill2Email	test@cmi.co.ma	itemnumber2	b1
BillToCity	Casablanca	itemnumber3	c1
BillToCompany	Billing Company	lang	en
BillToCountry	504	MaskedPan	400000***7190
BillToName	Bill John Doe	md	400000:BD64FA1BA77717 D21DA26554D2DE0 C9E65AB5D5872737AE720 F5D2484180228C: 4024:##6000000004
BillToPostalCode	12345	mdErrorMsg	
BillToStateProv	mystate	mdStatus	1
BillToStreet1	Address line 1	merchantID	6000000004
BillToStreet2	Address line 2	MERCHANTSURCHARGE	
BillToStreet3	Address line 3	noCallbackPaymentMethodList	
BillToTelVoice	123456	oid	sfgzzy4
CallbackResponse		okUrl	http://test.cmi.co.ma/ok
callbackUrl	http://test.cmi.co.ma/callback	PResSyntaxOK	
cardHolderName	Cardholder name	PResVerified	
cavv	AAABCRA0I1WFQDgnWDSX AAAAAAA=	paymentType	CARD
cavvAlgorithm		payResults.dsId	1
choix1	on	pMethod	
clientid	6000000004	price1	2.00
clientIp	81.192.141.16	price2	3.95
currency	504	price3	3.50
CUSTOMERSISDN		ProcReturnCode	0
CUSTOMERSURCHARGE		productcode1	a2
CVVPresence	1	productcode2	b2
desc1	desc1	productcode3	c2

desc2	desc2	qty1	3
desc3	desc3	qty2	1
digest	digest	qty3	5
DIMCRITERIA1		RecurringFrequency	
DIMCRITERIA10		RecurringFrequencyUnit	
DIMCRITERIA2		RecurringPaymentNumber	
DIMCRITERIA3		refreshtime	10
DIMCRITERIA4		Response	Approved
DIMCRITERIA5		ReturnOid	sfgzzy4
DIMCRITERIA6		rnd	lbJfQCTTrNRfMcNe111
DIMCRITERIA7		sessiontimeout	
DIMCRITERIA8		SettleId	1
DIMCRITERIA9		ShipToCity	Casablanca
dsId	1	ShipToCompany	Shipping Company
eci	5	ShipToCountry	504
Ecom_Payment_Card_ExpDate_Month	12	ShipToName	Ship John Doe
Ecom_Payment_Card_ExpDate_Year	17	ShipToPostalCode	12345
EDITABLEORDERITEM		ShipToStateProv	mystate
ErrMsg		ShipToStreet1	Address line 1
EXCHANGEAMOUNT	@@EXCHANGEAMOUNT@@	ShipToStreet2	Address line 2
EXCHANGECURRENCY		ShipToStreet3	Address line 3
EXTRA.CARDBRAND	VISA	ShipToTelVoice	789456
EXTRA.CARDISSUER	CDM	shopurl	http://test.cmi.co.ma/shop
EXTRA.HOSTMSG	APPROVED	SID	
EXTRA.TRXDATE	23/11/02017 15:57:06	storetype	3D PAY HOSTING
failUrl	http://test.cmi.co.ma/fail	total1	6.00
fatouratiExpress	1	total2	3.95
GRACEPERIOD		total3	17.50
hashAlgorithm	ver3	TRANID	129430
HostRefNum	732715056928	TransId	17327P7GH13718
id1	id1	trantype	PreAuth
id2	id2	txstatus	Y
id3	id3	vendorCode	
instalment		version	
		xid	7AFKUXDa5KeelWxM6wxfB9YfLDY=

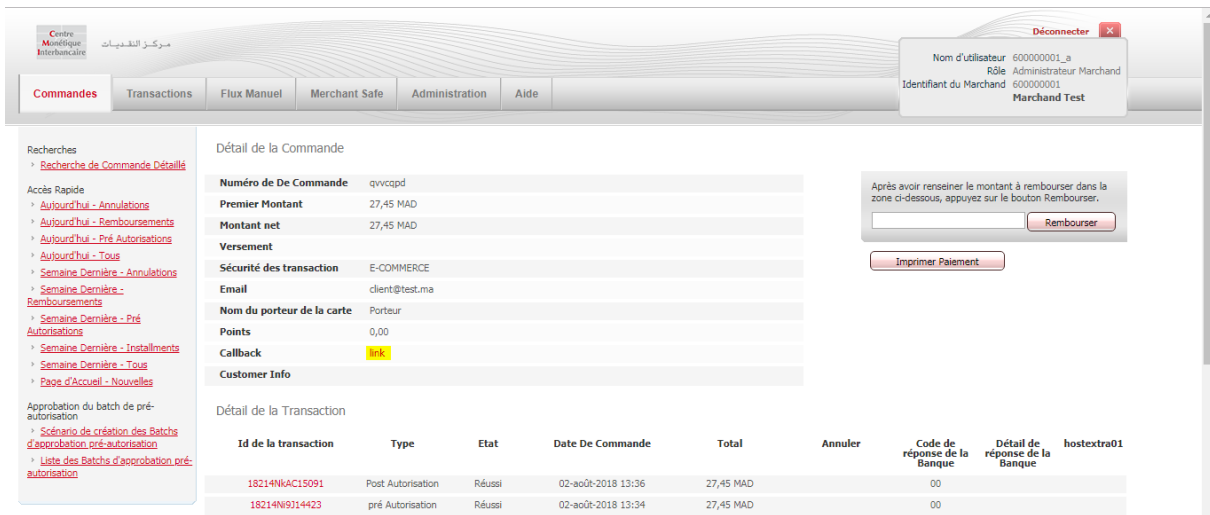
Cas de transaction échouée :

Parameter	Value	Parameter	Value
BillToCompany	Company	mdErrorMsg	Multiple values exist for the single parameter.

BillToName	Name	mdStatus	7
callbackUrl	http://test.cmi.co.ma/callback	oid	12345
clientid	600000000	okUrl	http://test.cmi.co.ma/ok
clientIp	1.1.1.1	price	
currency	504	ProcReturnCode	99
CVVPresence	1	productCode	
Ecom_Payment_Card_ExpDate_Month	1	qty	
Ecom_Payment_Card_ExpDate_Year	20	refreshtime	300
email	test@cmi.co.ma	ResponseError	
ErrCode	CORE-5110	retryXid	I6Hjx1K6zUGjqY98Z+vEnR2/gr4=
ErrMsg	Multiple values exist for the single paramater.	rnd	mmduZ3aMFe8qDmEG1MV1
failUrl	http://test.cmi.co.ma/fail	shopurl	http://test.cmi.co.ma/shop
hashAlgorithm	ver3	storetype	3d_pay_hosting
itemNumber		tel	600000000
lang	fr	total	
MaskedPan	400000***7190	trantype	PreAuth
		xid	I6Hjx1K6zUGjqY98Z+vEnR2/gr4=

4.2.6. Suivi des callbacks via le Merchant Center CMI

Le marchand a la possibilité de visualiser le détail de la requête du callback à travers son Merchant Center CMI où il a l'habitude de faire le suivi de ses transactions en ligne.



The screenshot shows the Merchant Center CMI interface. The top navigation bar includes 'Commandes', 'Transactions', 'Flux Manuel', 'Merchant Safe', 'Administration', and 'Aide'. The user is logged in as 'Marchand Test' with the role 'Administrateur Marchand'. The main content area displays 'Recherches' on the left and 'Détail de la Commande' on the right. The 'Détail de la Commande' section shows the following details:

- Numéro de De Commande:** qvccpd
- Premier Montant:** 27,45 MAD
- Montant net:** 27,45 MAD
- Versement:**
- Sécurité des transaction:** E-COMMERCE
- Email:** client@test.ma
- Nom du porteur de la carte:** Porteur
- Points:** 0,00
- Callback:** [link](#)
- Customer Info:**

Below the command details, there is a section for 'Détail de la Transaction' with a table showing transaction details:

Id de la transaction	Type	Etat	Date De Commande	Total	Annuler	Code de réponse de la Banque	Détail de réponse de la Banque	hostextra01
18214NkAC15091	Post Autorisation	Réussi	02-août-2018 13:36	27,45 MAD		00		
18214N9314423	pré Autorisation	Réussi	02-août-2018 13:34	27,45 MAD		00		

On the right side of the 'Détail de la Commande' section, there is a 'Rembourser' button and a note: 'Après avoir renseigné le montant à rembourser dans la zone ci-dessous, appuyez sur le bouton Rembourser.'

En cliquant sur le lien du Callback, dans le détail de la commande, on peut accéder au détail de la requête du callback échangée entre la plate-forme du CMI et le site web marchand.

Centre Mondiale Interbancaire

Comptes Rendus

Administration

Rechercher des retours marchands

Etat: -

Numéro de commande:

Date de début:

Date de fin:

Soumettre

Un article trouvé.

callbackIdNumber	Etat	Date de création	Date de la tentative suivante	Action	Action
38531	FINISHED	Thu Aug 02 13:35:00 WEST 2018	Thu Aug 02 13:35:00 WEST 2018	Reessayer	

Terminer tout RetryAll

Il faut cliquer sur l'identifiant du Callback en question pour pouvoir accéder au détail.

Centre Mondiale Interbancaire

Comptes Rendus

Administration

Rechercher des retours marchands

Numéro de De Commande: qvccpd

id: 38531

noCallbackPaymentMethodList

BillEmail: client@test.ma

clientid: 600000001

Ecom_Payment_Card_ExpDate_Year: 5

qty3: 1

qty2: 1

BillToCompany: Billing Company

ShipToCompany: Shipping Company

qty1: 3

BillToStreet3:

BillToStreet2:

BillToStreet1: Address

sessiontimeout:

BillToName: Client Name

CVVPresence: 1

EXCHANGE CURRENCY:

ShipToStreet3: Address line 3

itemnumber3: c1

ShipToStreet2: Address line 2

itemnumber2: b1

itemnumber1: a1

dstid: 0

choix1: on

DIMCRITERIA7: 789456

ShipToTelVoice: 6.00

total1: 3.95

DIMCRITERIA8: 17.50

DIMCRITERIA9:

total3:

ShipToStreet1: Address line 1

fatouratiExpress: 1

On peut ainsi visualiser l'ensemble des données envoyées par la plate-forme du CMI au site web marchand dans la requête du Callback.

status	NO
created	Thu Aug 02 12:35:00 WEST 2018
dimuid	600000001
Uri du callback	https://testpayment.cmi.co.ma/adapter/postauth.html
type	DIM_SYNC_CALLBACK
response	ACTION=POSTAUTH

On peut même voir la réponse du site marchand à la requête du Callback du CMI.

5. ETATS DES TRANSACTIONS

Le processus de paiement passe par plusieurs étapes durant lesquelles l'état de la transaction change. Dans ce chapitre, nous détaillons ce sujet avec des illustrations à partir du Merchant Center CMI qui est mis, par le CMI, à la disposition des marchands afin qu'ils puissent suivre leurs transactions en ligne à tout moment.

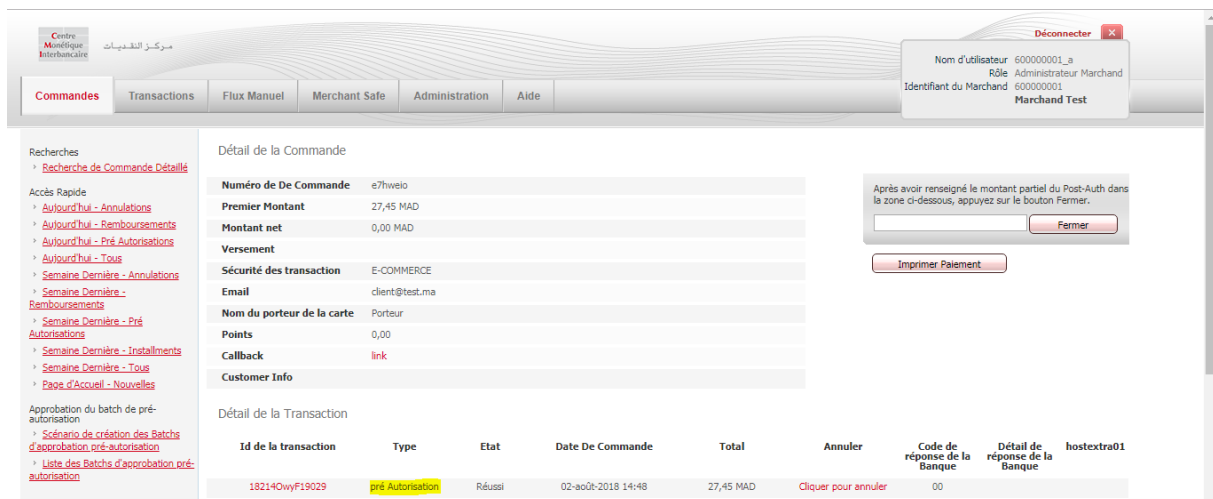
5.1. PRE AUTORISATION :

Lorsque le client saisit ses coordonnées bancaires dans la page de paiement, le CMI envoie une demande d'autorisation à la banque émettrice. Lorsque celle-ci accepte la demande, elle bloque le montant dans le compte bancaire du client. Dans ce cas, le client n'est pas débité. Il s'agit en effet d'un blocage de fonds qui garantit au marchand la récupération de ses fonds s'il accepte la transaction en question dans les délais autorisés (entre 4 et 7 jours).

Au niveau de la plate-forme CMI, la transaction est située dans la phase de Pré Autorisation. Ceci est visible via le Merchant Center CMI comme illustré ci-après.



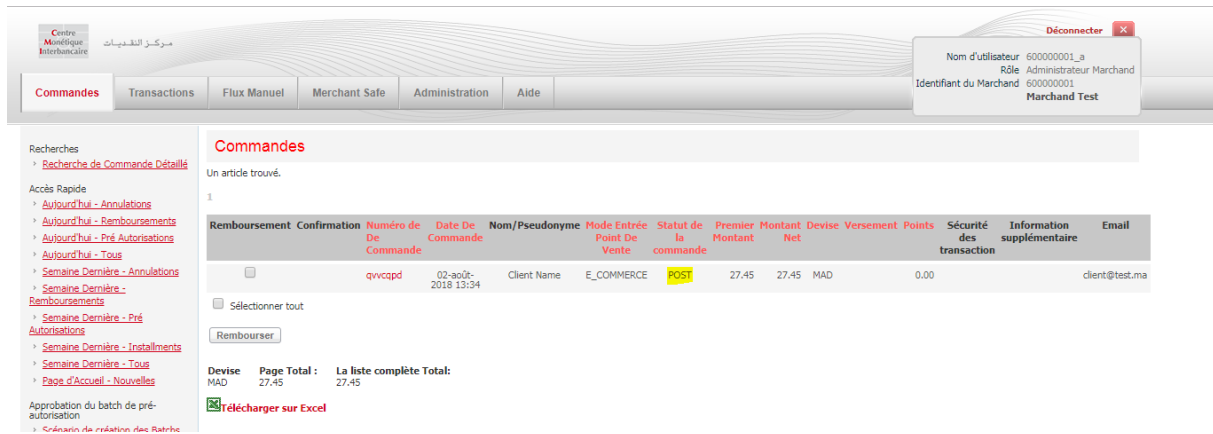
Le statut de la commande prend la valeur « PRE » qui fait référence à la Pré Autorisation.



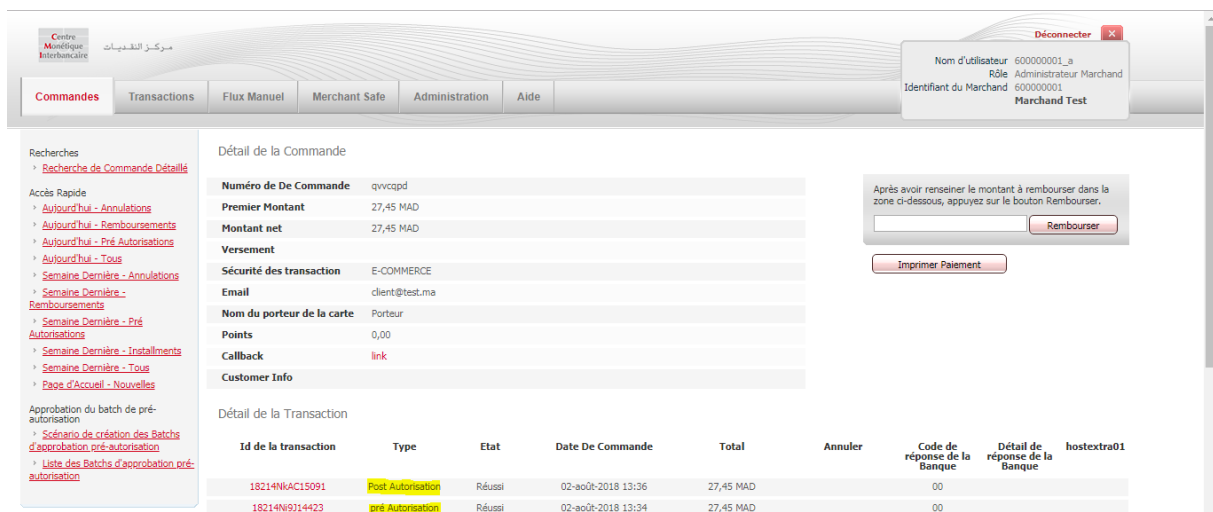
Dans le détail de la commande, nous trouvons une seule transaction de type « Pré Autorisation ».

5.2. POST AUTORISATION :

Lorsque la plate-forme CMI fait un callback au site marchand pour retourner le résultat de paiement, le site marchand demande le débit du client en répondant avec « ACTION=POSTAUTH ». Dans ce cas, la transaction passe à la phase de Post Autorisation. Ceci est visible via le Merchant Center CMI comme illustré ci-après.



Le statut de la commande prend la valeur « POST » qui fait référence à la Post Autorisation.



Dans le détail de la commande, nous trouvons deux transactions. L'une d'elles est de type « Pré Autorisation » et l'autre est de type « Post Autorisation ».

5.3. REMBOURSEMENT :

Des fois, le marchand souhaite rembourser un de ses clients suite à une transaction en ligne passée à travers son site web. Le marchand peut dans ce cas exécuter ce remboursement à travers son Merchant Center CMI. Une fois exécuté, la transaction passe à la phase de Remboursement. Ceci est visible via le Merchant Center CMI comme illustré ci-après.

Centre
Mondétique
Interbancaire

مركز التبادلات

Commandes

Transactions

Flux Manuel

Merchant Safe

Administration

Aide

Déconnecter

Nom d'utilisateur 600000001_a

Rôle Administrateur Marchand

Identifiant du Marchand 600000001

Marchand Test

Recherches

Recherche de Commande Détaillée

Accès Rapide

Aujourd'hui - Annulations

Aujourd'hui - Remboursements

Aujourd'hui - Pré Autorisations

Aujourd'hui - Tous

Semaine Dernière - Annulations

Semaine Dernière - Remboursements

Semaine Dernière - Pré Autorisations

Semaine Dernière - Installments

Commandes

Un article trouvé.

1

Remboursement	Confirmation	Numéro de Commande	Date De Commande	Nom/Pseudonyme	Mode Entrée Point De Vente	Statut de la commande	Premier Montant	Montant Net	Devises	Versement	Points	Sécurité des transaction	Information supplémentaire	Email
		qvcvcpd	02-août-2018 13:34	Client Name	E_COMMERCE	RFND	27,45	0,00	MAD		0,00			client@test.ma

Devises

MAD

0

Page Total :

0

La liste complète Total:

0

Télécharger sur Excel

Le statut de la commande prend la valeur « RFND » qui fait référence au Remboursement.

Centre
Mondétique
Interbancaire

مركز التبادلات

Commandes

Transactions

Flux Manuel

Merchant Safe

Administration

Aide

Déconnecter

Nom d'utilisateur 600000001_a

Rôle Administrateur Marchand

Identifiant du Marchand 600000001

Marchand Test

Recherches

Recherche de Commande Détaillée

Accès Rapide

Aujourd'hui - Annulations

Aujourd'hui - Remboursements

Aujourd'hui - Pré Autorisations

Aujourd'hui - Tous

Semaine Dernière - Annulations

Semaine Dernière - Remboursements

Semaine Dernière - Pré Autorisations

Semaine Dernière - Installments

Semaine Dernière - Tous

Page d'Accueil - Nouvelles

Détail de la Commande

Numéro de De Commande

qvcvcpd

Premier Montant

27,45 MAD

Montant net

0,00 MAD

Versement

Sécurité des transaction

E-COMMERCE

Email

client@test.ma

Nom du porteur de la carte

Porteur

Points

0,00

Callback

link

Customer Info

Détail de la Transaction

Id de la transaction	Type	Etat	Date De Commande	Total	Annuler	Code de réponse de la Banque	Détail de réponse de la Banque	hostextra01
18218KKA19413	Remboursement	Réussi	06-août-2018 10:09	27,45 MAD	Cliquer pour annuler	00		
18214NKA15091	Post Autorisation	Réussi	02-août-2018 13:36	27,45 MAD		00		
18214N9314423	pré Autorisation	Réussi	02-août-2018 13:34	27,45 MAD		00		

Dans le détail de la commande, nous trouvons trois transactions. La première est de type « Remboursement » et les deux autres sont de types « Pre Autorisation » et « Post Autorisation ».

5.4. ANNULATION :

Quand la transaction est à la phase « Pre Autorisation », le marchand peut précéder à son annulation pour demander le déblocage des fonds au niveau du compte bancaire du client. L'opération d'annulation peut se faire à travers le Merchant Center CMI. Ceci est visible via le Merchant Center CMI comme illustré ci-après.

Centre
Mondétique
Interbancaire

مركز التبادلات

Commandes

Transactions

Flux Manuel

Merchant Safe

Administration

Aide

Déconnecter

Nom d'utilisateur 600000001_a

Rôle Administrateur Marchand

Identifiant du Marchand 600000001

Marchand Test

Recherches

Recherche de Commande Détaillée

Accès Rapide

Aujourd'hui - Annulations

Aujourd'hui - Remboursements

Aujourd'hui - Pré Autorisations

Aujourd'hui - Tous

Semaine Dernière - Annulations

Semaine Dernière - Remboursements

Semaine Dernière - Pré Autorisations

Semaine Dernière - Installments

Commandes

Un article trouvé.

1

Remboursement	Confirmation	Numéro de Commande	Date De Commande	Nom/Pseudonyme	Mode Entrée Point De Vente	Statut de la commande	Premier Montant	Montant Net	Devises	Versement	Points	Sécurité des transaction	Information supplémentaire	Email
		e7hweio	02-août-2018 14:48	Client Name	E_COMMERCE	VOID	27,45	0,00	MAD		0,00			client@test.ma

Devises

MAD

0

Page Total :

0

La liste complète Total:

0

Télécharger sur Excel

Le statut de la commande prend la valeur « VOID » qui fait référence à l'annulation.

Centre
Mandataire
Interbancaire

مركز التجار

Déconnecter

Nom d'utilisateur: 600000001_a
Rôle: Administrateur Marchand
Identifiant du Marchand: 600000001
Marchand Test

Commandes
Transactions
Flux Manuel
Merchant Safe
Administration
Aide

Recherches

[Recherche de Commande Détaillée](#)

Accès Rapide

- [Autour d'Un - Annulations](#)
- [Autour d'Un - Remboursements](#)
- [Autour d'Un - Pré Autorisations](#)
- [Autour d'Un - Tous](#)
- [Semaine Dernière - Annulations](#)
- [Semaine Dernière - Remboursements](#)
- [Semaine Dernière - Pré Autorisations](#)
- [Semaine Dernière - Installments](#)
- [Semaine Dernière - Tous](#)
- [Page d'Accueil - Nouvelles](#)

Approbation du batch de pré-autorisation

- [Scénario de création des Batches d'approbation pré-autorisation](#)
- [Liste des Batches d'approbation pré-autorisation](#)

Détail de la Commande

Número de De Commande	e7hiveio
Premier Montant	27,45 MAD
Montant net	0,00 MAD
Versement	
Sécurité des transaction	E-COMMERCE
Email	client@test.ma
Nom du porteur de la carte	Porteur
Points	0,00
Callback	link
Customer Info	

Imprimer Paiement

Détail de la Transaction

Id de la transaction	Type	Etat	Date De Commande	Total	Annuler	Code de réponse de la Banque	Détail de réponse de la Banque	hostextra01
18214OwyF19029	pré Autorisation	Annuler	02-août-2018 14:48	27,45 MAD		00		

Dans le détail de la commande, nous trouvons une transaction de type « Pre Autorisation » à l'état « Annuler ».

Remarque:

- Pour plus d'informations sur les fonctionnalités du Merchant Center CMI, il faut consulter le manuel d'utilisation adéquat.

6. ANNEXE

6.1. Contact du service Intégration ECOM du CMI:

Si vous avez une question technique concernant l'interfaçage de votre site web avec la plateforme de paiement en ligne du CMI, vous pouvez contacter notre service Intégration ECOM via l'adresse email suivante :

integration.ecom@cmi.co.ma

6.2. Codes d'erreurs :

Le tableau suivant liste les principaux codes d'erreurs qui peuvent avoir lieu lors d'échecs de transactions. Ces codes d'erreurs font partie des données des transactions qui sont consultables via le Merchant Center CMI :

Error Code	System Error Message	Err Desc EN	Err Desc FR	Err Desc AR	Commentaire
99	3D-1004	Wrong security code	Code de sécurité erroné		Rejet de la plateforme à cause d'erreur de calcul du code de hachage. Ceci peut arriver soit au niveau de la requête de demande de paiement, soit dans la requête de confirmation de paiement.
99	3D-1005	Opertaion failor	Echec de l'opération		Rejet de la plateforme à cause d'échec d'authentification en ligne du client.
99	3D-1034	Opertaion failor	Echec de l'opération		Rejet de la plateforme à cause d'une fausse manipulation du client.
99	BM-1002	HOST based messaging problem	HOST based messaging problem	HOST	Message de réponse de l'acquéreur est invalide.
99	BM-9101	Failed operation	Opération échouée		Timeout avec l'interface d'acquisition.
99	BM-9102	Failed operation	Opération échouée		Timeout avec l'interface d'acquisition.
99	CORE-2010	The credit card is expired.	La carte de crédit est expirée		Rejet de la plateforme pour motif

					d'utilisation de carte de paiement expirée.
99	CORE-2012	The credit card number is not in a valid format.	Le format du numéro de carte de crédit n'est pas valide.		Rejet de la plateforme
99	CORE-2202	Failed operation	Opération échouée		Rejet de la plateforme dû à une règle de contrôle. Exemple de règles de contrôle : Demande d'autorisation en cas de fallback de l'authentification 3D Secure.
99	CORE-2208	Card brand is not allowed.	Marque de carte non autorisée.		Rejet de la plateforme
99	CORE-2253	The payment authorization could not be performed	Impossible de procéder à l'autorisation de paiement		Rejet de la plateforme dû à une règle de contrôle. Exemple de règles de contrôle : Utilisation d'une carte de paiement étrangère non authentifiable 3D Secure.
99	CORE-2515	Incorrect data	Données incorrectes		Rejet de la plateforme dû à des données erronées saisies par le client (exp. Format du CVV).
99	CORE-5110	Please return to the web site and try again	Merci de retourner au site web et réessayer		Rejet de la plateforme à cause d'une fausse manipulation du client.
99	RULE-0001	Your session has expired. Please return to the merchant website and try again.	Votre session a expiré. Merci de revenir au site marchand et réessayer.	.	CMI platform rejection due to session timeout.
99	RULE-0002	Cardholder authentication required	Authentification du porteur requise		CMI platform rejection due to cardholder authentication lack.
99	RULE-0003	Wrong card type	Type de carte erroné		CMI platform rejection due to wrong card type use.
99	RULE-0004	Card not allowed	Carte non permise		CMI platform rejection due to not allowed card use.
03	ISO8583-03	Payment authorization not permitted for this merchant	Autorisation de paiement non permise pour ce marchand		Rejet de la banque

04	ISO8583-04	Payment authorization rejected with this card	Autorisation de paiement rejetée avec cette carte		Rejet de la banque pour motif d'utilisation de carte de paiement volée.
05	ISO8583-05	Payment authorization declined	Autorisation de paiement non acceptée		Rejet de la banque sans précision du motif.
12	ISO8583-12	Payment authorization rejected	Autorisation de paiement rejetée		Rejet de la banque
13	ISO8583-13	INVALID AMOUNT	Montant non valide		Rejet de la banque
14	ISO8583-14	Payment authorization rejected with the used card	Autorisation de paiement rejetée avec la carte utilisée		Rejet de la banque
15	ISO8583-15	Payment authorization failed	Autorisation de paiement échouée		Rejet de la banque
39	ISO8583-39	No credit account	Pas de compte de crédit		Rejet de la banque
51	ISO8583-51	Insufficient funds.	Solde de la carte insuffisant		Rejet de la banque
54	ISO8583-54	Payment authorization rejected with this card	Autorisation de paiement rejetée avec cette carte		Rejet de la banque pour motif d'utilisation de carte de paiement expirée ou erreur de saisie de la date d'expiration de la carte.
57	ISO8583-57	Payment authorization not permitted	Autorisation de paiement non permise		Rejet de la banque
61	ISO8583-61	Activity amount limit exceeded.	Plafond dépassé		Rejet de la banque
62	ISO8583-62	Payment authorization rejected with this card	Autorisation de paiement rejetée avec cette carte		Rejet de la banque
63	ISO8583-63	Payment authorization rejected with this card	Autorisation de paiement rejetée avec cette carte		Rejet de la banque pour des raisons de sécurité.
65	ISO8583-65	Activity limit exceeded.	Plafond dépassé		Rejet de la banque
82	ISO8583-82	CVV Failure or CVV Value supplied is not valid.	Echec CVV ou valeur CVV fournie non valide.		Rejet de la banque
86	ISO8583-86	Payment authorization rejected	Autorisation de paiement rejetée		Rejet de la banque
90	ISO8583-90	Payment authorization rejected	Autorisation de paiement rejetée		Rejet de la banque
91	ISO8583-91	Payment authorization failed	Autorisation de paiement échouée		Timeout avec l'interface de la banque.
96	ISO8583-96	Payment authorization failed	Autorisation de paiement échouée		Le traitement de l'opération a échoué

Remarque:

- Les développeurs web rencontrent souvent l'erreur 3D-1004 lors de leurs premiers tests d'intégration. Dans ce cas, l'origine de l'erreur provient en général du fait que le développeur oublie de renseigner sa clé secrète de hachage au niveau du Merchant Center CMI. La procédure de renseignement de la clé secrète de hachage est précisé dans le kit d'intégration du CMI.