

Monetico Paielement

Paielement sécurisé sur Internet

**Paielement express multiCB :
Service de gestion de cartes -
Documentation technique**



SOMMAIRE

1	Introduction	3
1.1	Principe	3
1.2	Clé de sécurité commerçant	3
2	Spécifications des messages échangés	4
2.1	Appel du module de gestion de cartes	4
2.1.1	Calcul du sceau	4
2.1.2	Exemples de requête	5
2.2	Réponse du module de gestion de cartes	6
2.2.1	Liste des valeurs du code retour dans les messages JSON	7
2.2.2	Exemple de retour JSON du service	8
3	Utilisation du service	9
3.1	En Test	9
3.2	En production	9
3.3	Assistance technique	9
4	Aides à l'installation	9
4.1	Les problèmes les plus fréquents	9
4.1.1	Problème de calcul du sceau de sécurité	9

1 Introduction

1.1 Principe

Le but du module « Gestion de portefeuille de cartes » est de permettre aux commerçants de lister, modifier ou supprimer des cartes bancaires séquestrées dans un portefeuille de carte. Ce module est utilisable uniquement par les commerçants ayant souscrit à l'option Paiement Express.

1.2 Clé de sécurité commerçant

Une clé de sécurité, propre à chaque TPE, destinée à certifier les données échangées entre le serveur du commerçant et le serveur de paiement sécurisé de la banque, est indispensable pour utiliser le service de paiement par carte bancaire. Un lien, permettant de télécharger cette clé de sécurité, est envoyé par notre centre de support au commerçant.

Le commerçant peut demander la génération d'une nouvelle clé, périodiquement ou à l'occasion d'évènements tels qu'une mise en production, un changement d'hébergeur, un changement de prestataire, etc.

Il est de la responsabilité du commerçant de conserver cette clé de façon sûre et confidentielle en exploitant les meilleurs outils disponibles dans son environnement.

La clé de sécurité est représentée de façon externe par 40 caractères hexadécimaux (par exemple : 0123456789ABCDEF0123456789ABCDEF01234567).

Cette représentation externe doit être convertie en une chaîne de 20 octets (représentation opérationnelle) avant utilisation.

2 Spécifications des messages échangés

2.1 Appel du module de gestion de cartes

Les informations de la demande sont envoyées au serveur de la banque par un message HTTPS (TLS). L'application du commerçant doit émettre une requête en méthode POST à destination du service de gestion de cartes sur les serveurs de la banque.

Champs	Description	Remarque
version	Version du service utilisée	Version actuelle 3.0
tpe	Numéro de TPE Virtuel du commerçant. Taille : 7 caractères	Exemple : 1234567
action	Action à effectuer sur le portefeuille ou la carte.	
aliascb	Alias donné au portefeuille lors de la séquestration	
mac	Sceau issu de la certification des données	Taille : 40 caractères hexadécimaux
identifiant_carte	Identifiant de la carte séquestrée.	Correspond au hash de la carte renvoyé dans l'appel à l'interface retour. Pas nécessaire pour le service de listage de cartes.
nom_carte	Nom de la carte séquestrée	Utilisable uniquement pour la modification d'une carte (action « modifier_carte »)

Liste des actions disponibles :

Valeur du champ « action »	Description
desactiver_carte	Permet de supprimer une carte bancaire du portefeuille de carte.
modifier_carte	Permet de modifier le nom attribué à une carte bancaire
positionner_carte_default	Permet de positionner une carte bancaire par défaut. La carte par défaut est la carte qui sera présélectionnée lors de l'affichage de la page de paiement.
lister_cartes	Permet de lister les cartes bancaires présentes dans un portefeuille.

2.1.1 Calcul du sceau

Le sceau (à mettre dans le champ MAC) est calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.

Cette fonction générera le sceau à partir de données à certifier et de la clé de sécurité commerçant sous sa forme opérationnelle.

Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations du formulaire :

<version>*<tpe>*<aliascb>*<action>*<identifiant_carte>*

Exemple pour une demande :

3.0*1234567*portfeuille1*lister_cartes*
707f9d31a99a1d8980aab4ae54f62086200f1b0b*

2.1.2 Exemples de requête

- Lister les cartes bancaires d'un portefeuille

```
<form method="post" name="GestionPortfeuilleFormulaire" target="_top" action="https://p.monetico-
services.com/gestion_aliascb.cgi">
  <input type="hidden" name="version" value="3.0">
  <input type="hidden" name="tpe" value="1234567">
  <input type="hidden" name="action" value="lister_cartes">
  <input type="hidden" name="aliascb" value="portfeuille1">
  <input type="hidden" name="mac" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
</form>
```

- Modifier le nom associé à une carte bancaire

```
<form method="post" name="GestionPortfeuilleFormulaire" target="_top" action="https://p.monetico-
services.com/gestion_aliascb.cgi">
  <input type="hidden" name="version" value="3.0">
  <input type="hidden" name="tpe" value="1234567">
  <input type="hidden" name="action" value="modifier_carte">
  <input type="hidden" name="aliascb" value="portfeuille1">
  <input type="hidden" name="mac" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
  <input type="hidden" name="identifiant_carte" value="707f9d31a99a1d8980aab4ae54f62086200f1b0b">
  <input type="hidden" name="nom_carte" value="Compte commun">
</form>
```

2.2 Réponse du module de gestion de cartes

Le module « Gestion de portefeuille de carte » renvoie au commerçant un message au format JSON.

Voici la description des balises des messages JSON renvoyés au commerçant

Balise		Description	Remarque
cdr		Code retour	
defaultCard		Carte bancaire par défaut du portefeuille.	Absent si action=modifier_carte
deletedCard		Carte supprimée suite à l'appel du service « Gestion de portefeuille de carte »	Uniquement si action=desactiver_carte
cards	expMonth	Mois d'expiration de la carte bancaire	Uniquement si action=lister_cartes
	expYear	Année d'expiration de la carte bancaire	
	hiddenNumber	Numéro de la carte bancaire au format PCIDSS. Exemple : 000001XXXXXX0005	
	id	Identifiant de la carte bancaire. Il s'agit du hash de la carte renvoyé lors de l'appel à l'interface retour	
	isExpired	« false » si la carte bancaire est expirée, « true » sinon.	
	name	Nom associé à la carte bancaire.	
	origin	Pays d'origine de la carte bancaire. Exemple : FRA	
modifiedCard		Identifiant de la carte bancaire modifiée	Uniquement si action=modifier_carte
newName		Nouveau nom associé à la carte bancaire	

2.2.1 Liste des valeurs du code retour dans les messages JSON

Valeur balise cdr	Description	Commentaire
0	Action réussie	
-100	Problème technique	Problème technique, il faut réitérer la demande et contacter le support Monetico Paiement en cas de nouvel échec.
-101	Méthode d'appel incorrecte	Le MAC n'est pas présent dans l'appel.
-110	Version incorrecte	Version différente de 3.0
-111	TPE non existant	Le terminal de paiement virtuel n'existe pas. Vérifier la valeur présente dans le champ tpe.
-112	Portefeuille/Alias non existant	Le portefeuille n'existe pas. Vérifier la valeur présente dans le champ aliascb
-113	Action inconnue	La valeur du champ action ne correspond pas à une des actions réalisables sur le portefeuille de cartes.
-114	Mac Incorrect	Le MAC est incorrect.
-115	Version mal formée	Le contenu du champ version ne vérifie pas le format requis.
-116	TPE mal formé	Le contenu du champ tpe ne vérifie pas le format requis.
-117	Alias mal formé	Le contenu du champ aliascb ne vérifie pas le format requis.
-118	Action mal formée	Le contenu du champ action ne vérifie pas le format requis.
-119	Mac mal formé	Le contenu du champ mac ne vérifie pas le format requis.
-120	Identifiant carte mal formé	Le contenu du champ identifiant_carte ne vérifie pas le format requis.
-121	Identifiant de carte inconnue	La carte bancaire n'est pas présente dans le portefeuille de cartes.
-122	Nom mal formé	Le contenu du champ nom_carte ne vérifie pas le format requis.
-201	Carte bancaire expirée	Impossible de modifier la carte bancaire car elle est expirée

-202	Suppression de la carte bancaire non autorisée	Impossible de supprimer la carte bancaire
-205	Portefeuille vide	Le portefeuille de carte est vide
-207	Carte bancaire déjà positionnée par défaut	Lors d'une demande de positionnement d'une carte bancaire par défaut alors que celle-ci est déjà la carte par défaut.

2.2.2 Exemple de retour JSON du service

- Réponse à une demande de listage des cartes bancaires d'un portefeuille

```
{
  "cards":
  [
    {
      "expMonth": "12",
      "expYear": "2019",
      "hiddenNumber": "000003XXXXXXXX0005",
      "id": "86e39e91a37e7bbd8b4d04d105912b3b8453092c",
      "isExpired": false,
      "name": "",
      "origin": "FRA"
    },
    {
      "expMonth": "12",
      "expYear": "2019",
      "hiddenNumber": "000001XXXXXXXX0005",
      "id": "707f9d31a99a1d8980aab4ae54f62086200f1b0b",
      "isExpired": false,
      "name": "Ma Carte",
      "origin": "FRA"
    }
  ],
  "cdr": 0,
  "defaultCard": "86e39e91a37e7bbd8b4d04d105912b3b8453092c"
}
```

- Réponse à une demande de modification du nom associé à une carte bancaire

```
{
  "cdr": 0,
  "modifiedCard": "707f9d31a99a1d8980aab4ae54f62086200f1b0b",
  "newName": "Ma Carte perso"
}
```

- Réponse à une demande de positionnement par défaut d'une carte bancaire

```
{
  "cdr": 0,
  "defaultCard": "707f9d31a99a1d8980aab4ae54f62086200f1b0b"
}
```

- Réponse à une demande de suppression d'une carte bancaire

```
{
  "cdr":0,
  "defaultCard":"707f9d31a99a1d8980aab4ae54f62086200f1b0b",
  "deletedCard":"86e39e91a37e7bbd8b4d04d105912b3b8453092c"
}
```

3 Utilisation du service

3.1 En Test

Le rôle de notre serveur de test est de vous permettre de tester et de valider vos développements.

L'environnement de test est disponible à l'adresse suivante :

- https://p.monetico-services.com/test/gestion_aliascb.cgi

3.2 En production

Après avoir validé vos développements, vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

- https://p.monetico-services.com/gestion_aliascb.cgi

3.3 Assistance technique

Euro Information propose une assistance à la compréhension générale de l'utilisation de sa solution :

- Par courriel : en écrivant un message à la boîte aux lettres « **Commerce Electronique** »
 - Crédit Mutuel : centrecom@e-i.com
 - CIC : centrecom@e-i.com
- Par téléphone : en appelant le **0820 821 735**

Cependant, Euro Information n'assure pas de support concernant les problématiques d'intégration technique de sa solution de paiement dans le système d'information commerçant.

4 Aides à l'installation

4.1 Les problèmes les plus fréquents

4.1.1 Problème de calcul du sceau de sécurité

Message d'erreur

```
{
  "cdr":-114
}
```

Causes possibles

- Le formulaire que vous nous avez envoyé ne contient pas toutes les informations requises
- Le calcul du sceau MAC est erroné
- Le calcul du sceau MAC est effectué avec une mauvaise clé

Résolution du problème

Suivez scrupuleusement le cheminement décrit ci-dessous ; à la fin de chaque étape pour laquelle vous avez effectué des changements dans votre implémentation, effectuez de nouveaux tests de paiement. S'ils ne sont pas fructueux, passez à l'étape suivante.

Attention : ne sautez pas d'étape !

Etape 1 : vérifiez que toutes les variables envoyées dans le formulaire sont présentes, correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.

Etape 2 : vérifiez que vous avez réussi à éviter les erreurs inhérentes à certains champs particuliers :

- la valeur MAC correspond-elle à une chaîne de 40 caractères hexadécimaux (valeurs autorisées : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) ?
- la valeur de la variable `identifiant_carte` est-elle bien une chaîne ne contenant que des lettres (non accentuées) et des chiffres ?

Etape 3 : vérifiez que la chaîne sur laquelle vous calculez le sceau MAC respecte le formalisme décrit précédemment, à savoir :

`<version>*<tp>*<aliascb>*<action>*<identifiant_carte>*`

Soyez particulièrement attentif au fait que les données utilisées doivent être les mêmes que celles que vous fournissez dans le formulaire de paiement ; le meilleur moyen pour atteindre cet objectif est de stocker à l'avance les différentes informations, puis d'utiliser ce stockage pour le calcul du sceau MAC et pour la construction du formulaire. Au contraire, renseigner les données à la volée peut induire des différences entre celles utilisées pour le calcul du sceau et celles utilisées pour la construction du formulaire (par exemple, pour le champ `date`, il peut y avoir une différence de quelques secondes).

Etape 4 : vérifiez que vous utilisez la bonne clé :

- vous devez utiliser la dernière clé qui vous a été fournie par nos services,
- vérifiez que la clé correspond à votre algorithme de calcul de sceau (SHA1 ou MD5),
- Contactez notre service de support et demandez-leur de valider avec vous que vous utilisez bien la bonne clé

Si malgré toutes ces vérifications vous obtenez toujours ce message d'erreur, le problème réside dans l'intégration de notre solution dans votre système d'information.

La grande diversité des langages et des spécificités liées à l'environnement utilisés pour l'implémentation de notre solution de paiement, sont autant de paramètres dont nous ne

maîtrisons pas tous les aspects et par conséquent, ils ne nous permettent pas de vous fournir un support personnalisé plus ample.