Monetico Paiement

Paiement sécurisé sur Internet

Documentation Générale

EURO INFORMATION

SOMMAIRE

1 Présentation

Monetico Paiement est une solution qui permet à vos clients de vous régler par carte bancaire, sur votre site internet. Véritable terminal de paiement électronique (TPE) virtuel, il s'adapte aussi facilement à un petit commerce en ligne qu'à un site d'e-commerce international travaillant en plusieurs langues et devises.

Ce service, opérationnel depuis 1996, décharge votre site de toute la phase de paiement ; en effet cette dernière a lieu directement sur le serveur de paiement sécurisé de la banque.

Le serveur de paiement effectue la vérification de la validité de la carte bancaire de l'acheteur avant d'accorder l'autorisation de paiement et confirme automatiquement le résultat de la demande de paiement au serveur du commerçant.

Les éléments de sécurisation des échanges mis en œuvre dans le cadre du service de paiement sécurisé sont les suivants :

- intégrité des données échangées entre le serveur du commerçant et le serveur de la banque assurée par une méthode de scellement,
- authentification du commerçant émetteur de la demande de paiement,
- confidentialité des données échangées entre l'acheteur et le serveur de paiement de la banque (numéro, date de validité et cryptogramme visuel de la carte bancaire) assurée par chiffrement TLS,
- saisie directe des coordonnées Carte Bancaire sur le site sécurisé de la banque, garantissant que ni le commerçant, ni aucun intermédiaire technique, n'auront connaissance des informations concernant la carte bancaire,
- intégration native de la fonctionnalité Visa 3D Secure / MasterCard Secure Code, qui permet à la banque de garantir le paiement dans les pays où la solution est déployée.

Notre solution de paiement offre depuis son introduction la meilleure sécurisation possible ; cette sécurisation est garantie par des audits réguliers réalisés par des sociétés indépendantes.

De plus, l'utilisation d'une solution « Open Source » vous permet une maîtrise complète et transparente. Vous pourrez donc mettre en œuvre selon vos propres préférences et constater par vous-même et en toute transparence le niveau de sécurité de notre solution. Ceci vous permettra également d'être en permanence à jour en incluant dans votre solution les dernières mises à jour de sécurité disponibles.

1.1 Principe

La solution Monetico Paiement s'intègre facilement dans votre site internet, quelle que soit sa configuration. Les paiements par carte bancaire de vos clients transitent alors par votre banque, qui enregistre pour vous les transactions.

Les différentes étapes lors d'un paiement

Les contrôles portent notamment sur :

- la validité du numéro de carte
- le cryptogramme visuel
- la date de validité de la carte
- le fichier des oppositions
- l'encours carte
- l'identité du porteur

Vous bénéficiez d'un retour d'information immédiat sur votre serveur suite à chaque paiement effectué sur notre plate-forme, vous notifiant du succès ou de l'échec du paiement. En complément, nous pouvons également vous notifier par courriel du résultat de ces paiements.

1.2 Vendre à l'international

Vous voulez vendre à l'international ? Monetico Paiement accepte les cartes bancaires nationales et internationales des réseaux :

- Carte Bleue / Visa
- MasterCard
- American Express[1]

Pour faciliter le paiement par vos clients étrangers, les pages de paiement sont disponibles dans 9 langues :

- Français
- Anglais
- Allemand
- Italien
- Espagnol
- Néerlandais
- Portugais
- Suédois
- Japonais

Notre plate-forme autorise, en plus de l'euro, les règlements[2] en :

- dollars
- livres anglaises
- yens
- francs suisses
- devises nordiques out
- etc.

[1] *Pour ce type de carte vous devez signer un contrat auprès d'American Express*
[2] *Sous réserve de conclusion des contrats de gestion des devises correspondantes*

1.3 Description de la phase paiement

L'acheteur arrive sur le site sécurisé de la banque après avoir cliqué sur le bouton « paiement par carte bancaire » du site du commerçant :

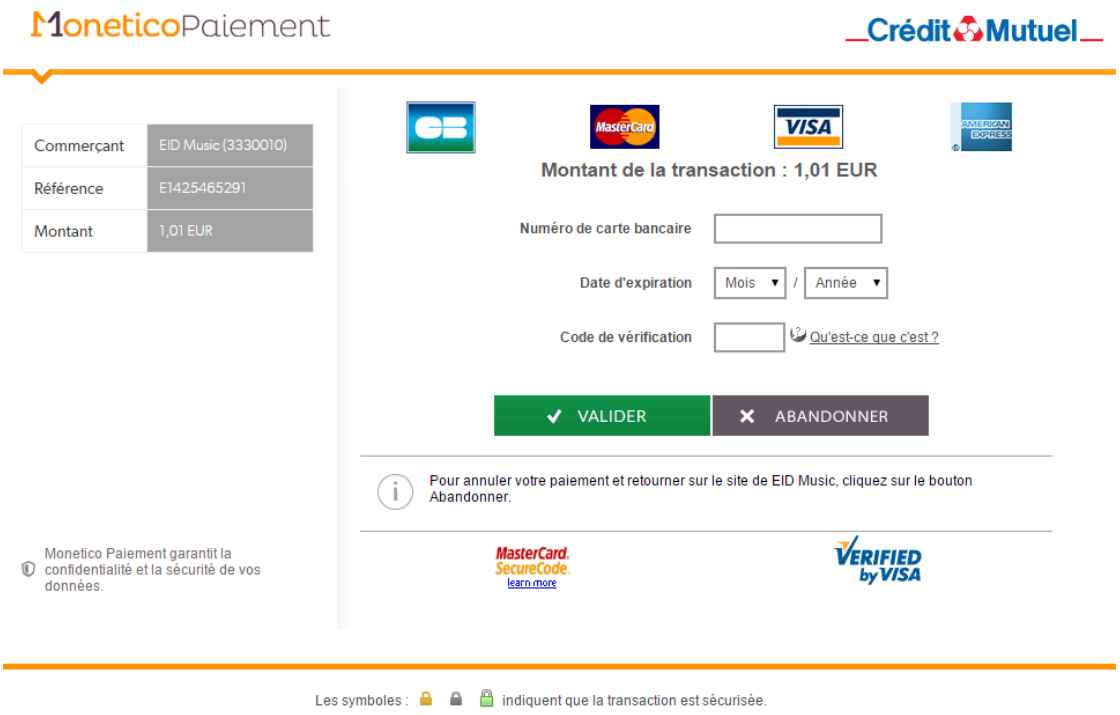


Figure 1 : écran de saisie des informations de la carte bancaire

Le client peut voir en permanence le nom et l'identifiant du commerçant, ainsi que la référence de la transaction.

Il est possible de personnaliser les pages de paiement avec le logo du commerçant (image GIF de 120 Pixels * 120 Pixels maxi). Il suffit pour cela de fournir l'URL de l'image GIF téléchargeable, située sur le serveur du commerçant.

L'acheteur entre son numéro de carte bancaire, la date de validité et le cryptogramme visuel situé au dos de sa carte, puis clique sur le bouton « valider » :

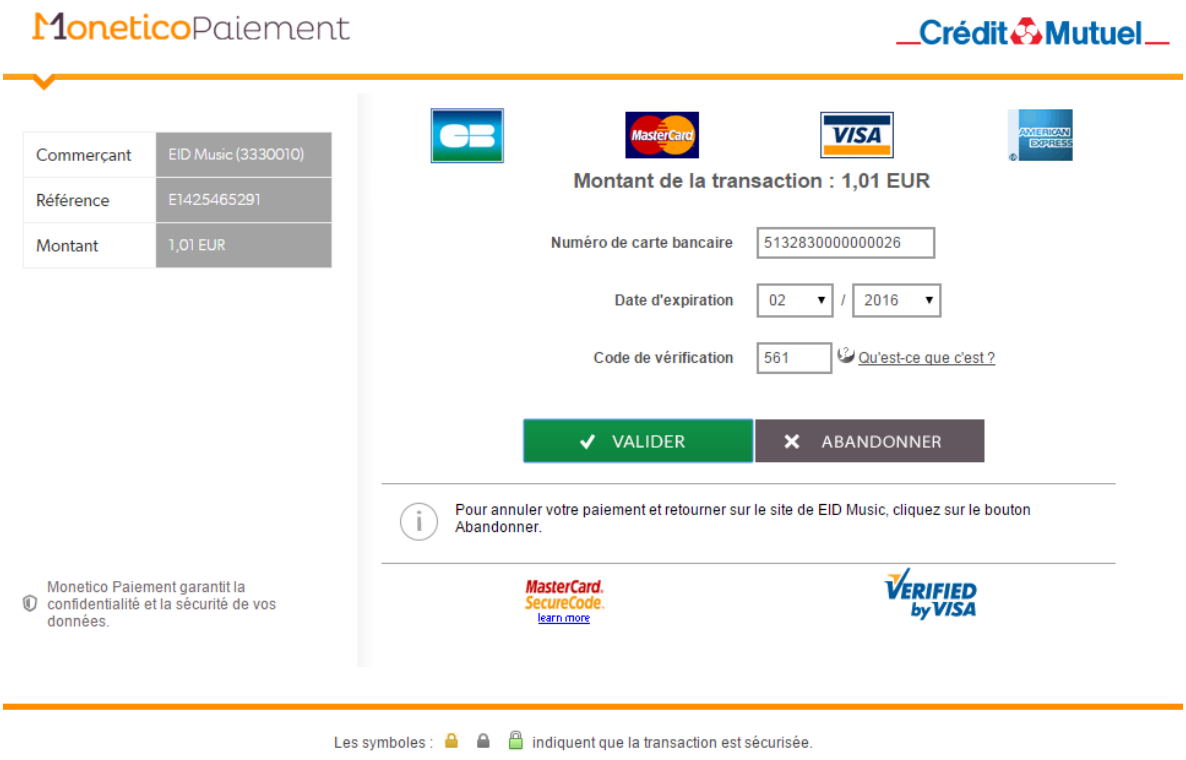


Figure 2 : écran de saisie des informations de la carte bancaire

A l'issue du paiement, le site sécurisé de la banque affiche :

- **Un ticket récapitulatif** contenant les informations essentielles de la transaction (montant, devise, date et heure, numéro d'autorisation) permettant à l'acheteur de conserver une trace de la transaction (sous réserve d'impression par ses soins) ;
- **Un lien** (dont le texte est personnalisable), qui permet à l'acheteur de retourner sur le site du commerçant

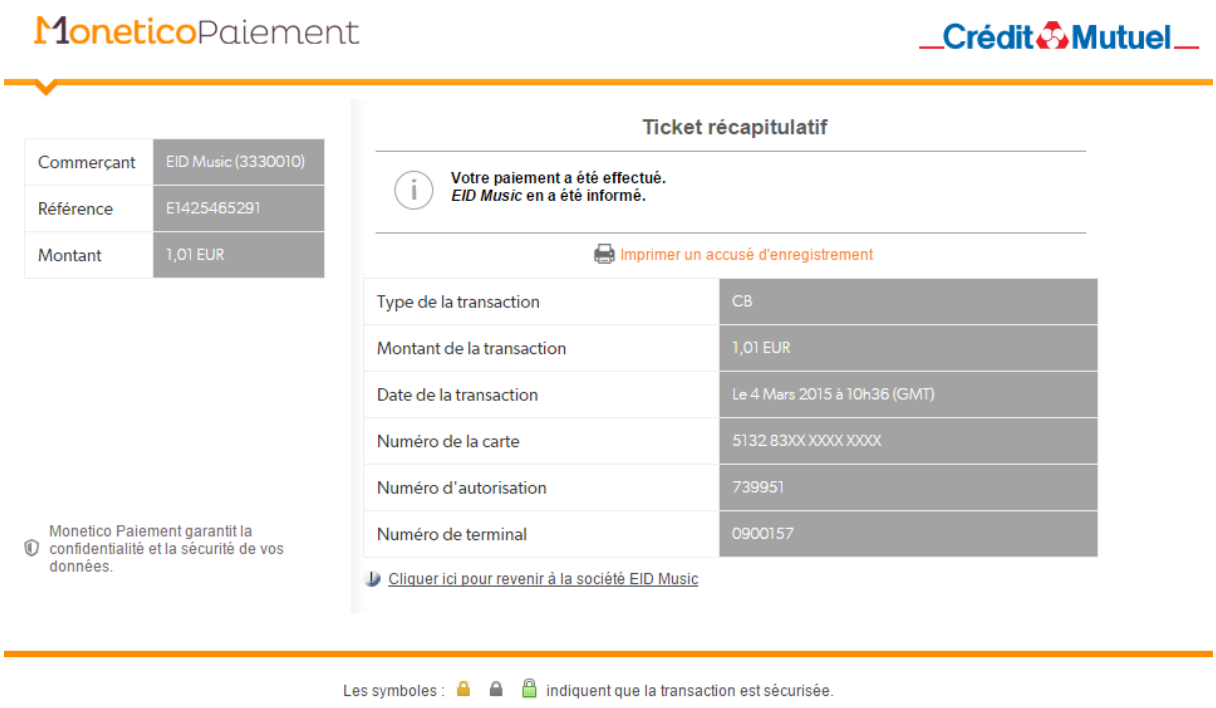


Figure 3 : écran récapitulatif du paiement

1.4 Suivi des paiements par le commerçant

Pour traiter vos transactions, nous mettons à votre disposition un gestionnaire commerçant, véritable tableau de bord des commandes enregistrées sur votre site.

Votre gestionnaire commerçant vous propose 4 groupes de fonctionnalités :

- **La gestion des transactions** : encaissement (partiel, total, différé), annulation d'une transaction ou remboursement (partiel ou total).
- **L'historique** : liste des transactions enregistrées sur six mois glissants, détails de chaque transaction, téléchargement de l'historique, visualisation des impayés.
- **Le paramétrage** : paramétrage du reporting de l'activité quotidienne, paramétrage du module anti-fraude
- **La saisie d'opération** : vous saisissez directement des commandes effectuées sur un autre canal (courrier ou téléphone) avec les mêmes contrôles sur la carte bancaire. Cette fonctionnalité optionnelle n'est disponible que pour certaines activités.

1.5 Modes de fonctionnement du paiement

Six modes de fonctionnement sont offerts ; ces modes sont exclusifs l'un de l'autre sur un même Terminal : un TPE fonctionne dans un seul mode (inscrit au contrat) :

- **Paiement immédiat**
- **Paiement différé**
- **Paiement partiel**
- **Paiement récurrent (abonnement)**
- **Paiement fractionné**
- **Paiement aggregé**

1.5.1 Paiement immédiat

La demande d'autorisation du paiement est effectuée en direct à la commande; si l'autorisation est délivrée, la mise en recouvrement est faite immédiatement. Dans ce mode, il n'y a pas possibilité d'annulation du paiement.

Ce mode de paiement est compatible avec l'authentification 3D Secure.

1.5.2 Paiement différé

La demande d'autorisation du paiement est effectuée en direct à la commande; la mise en recouvrement n'est pas déclenchée automatiquement, elle est différée. Elle peut être déclenchée à n'importe quel moment dans un délai paramétrable entre 0 et 7 jours ouvrés.

Dans ce mode, le commerçant peut consulter sur son tableau de bord, pendant ce délai, la liste des paiements différés en attente de mise en recouvrement.

La mise en recouvrement peut être faite par le commerçant via son tableau de bord ou via le WebService de capture.

Le commerçant peut également opter s'il le souhaite pour une mise en recouvrement automatique (effectuée par nos serveurs) à la fin de la période de différé. Si cette option n'est pas activée, et que le commerçant n'a pas demandé la mise en recouvrement du paiement au cours du délai de différé, alors la demande de paiement est abandonnée et ne pourra plus être recouvrée.

Ce mode de paiement est compatible avec l'authentification 3D Secure.

Remarque : Si une mise en recouvrement est demandée un samedi (automatiquement, ou manuellement via le tableau ou via le WebService de capture), celle-ci ne sera effective que le lundi suivant.

Exemple :

Votre TPE est configuré en paiement différé 2 jours mise en recouvrement automatique. Vous recevez un paiement le jeudi, il ne sera mis en recouvrement que le lundi suivant.

1.5.3 Paiement partiel

Le principe de ce mode de paiement est de permettre au commerçant de mettre en recouvrement le montant de la commande en plusieurs fois, par exemple si la livraison se fait en plusieurs parties.

Quand le client effectue la demande de paiement, une vérification de la validité de la carte est effectuée, mais aucune demande d'autorisation n'est émise. Le commerçant dispose alors d'un délai paramétrable de 8 à 120 jours pour effectuer une ou plusieurs demandes de mise en recouvrement. Ces demandes peuvent être faites soit via le tableau de bord commerçant, soit via le WebService de capture. Chaque demande de mise en recouvrement sera automatiquement accompagnée d'une demande d'autorisation; il est donc possible que la demande de mise en recouvrement soit refusée.

Dans ce mode, le commerçant peut consulter, sur son tableau de bord, la liste des paiements partiels en attente de traitement. A la fin de la période de différé, les montants non mis en recouvrement sont annulés.

Ce mode de paiement n'utilise pas l'authentification 3D Secure.

1.5.4 Paiement récurrent (abonnement)

Le paiement récurrent permet de reproduire une commande existante avec une fréquence donnée (sur une base mensuelle). Chaque mensualité se comporte comme un paiement partiel (voir paragraphe précédent).

Le commerçant peut paramétrer :

- le jour du renouvellement : soit un jour donné du mois, soit à la date anniversaire de la commande,
- la périodicité : mensuelle, trimestrielle, ...
- le nombre maximal de renouvellements
- Le type de mise en recouvrement pour chaque récurrence :
  - automatique le jour du renouvellement,
  - automatique le dernier jour de la récurrence (si aucune mise en recouvrement manuelle n'a été faite au cours de la récurrence),
  - aucune : dans ce cas, la gestion de la mise en recouvrement est à la charge du commerçant

Remarque : *ces actions automatiques ne sont pas effectuées sur la première mensualité qui doit faire l'objet d'un traitement manuel de la part du commerçant.*

Remarque : *Le commerçant garde la possibilité de stopper la récurrence d'une commande à tout moment par le biais de son tableau de bord ou du WebService de capture.*

Un récapitulatif des nouvelles mensualités est fourni au commerçant à la fin de chaque période de renouvellement.

Ce mode de paiement n'utilise pas l'authentification 3D Secure.

1.5.5 Paiement fractionné

Le paiement fractionné permet de débiter automatiquement un client en plusieurs fois : la demande de paiement est fractionnée en plusieurs demandes de paiement. C'est une facilité de paiement pour le client, mais **ce n'est pas un crédit** : le commerçant est crédité en plusieurs fois également, il ne perçoit pas le montant total dès la demande de paiement.

Le commerçant peut paramétrer le nombre d'échéances mensuelles : 2, 3 ou 4. Le renouvellement des échéances peut se faire soit à date anniversaire de la commande, soit un jour fixe (le 02 pour les commandes passées entre le 1er et le 20, le 15 pour les commandes passées entre le 21 et la fin du mois).

Le commerçant peut également personnaliser le montant de chaque échéance : soit un pourcentage différent à chaque fraction (par exemple acompte-solde), soit proportionnel au nombre d'échéances,

Remarque : *Le commerçant garde la possibilité de piloter les dates et montants des échéances lors de chaque paiement via la requête envoyée.*

La première échéance se comporte comme un paiement différé : une demande d'autorisation est effectuée lors de la prise de commande. La mise en recouvrement de la première échéance suit les principes décrits précédemment pour le paiement différé.

Pour les échéances suivantes, une demande d'autorisation est effectuée à chaque mise en recouvrement. En cas de refus d'autorisation (4 tentatives sont faites, à plusieurs jours d'intervalle), le commerçant peut choisir d'annuler les échéances restantes ou de reporter le montant de l'échéance en cours sur l'échéance suivante.

En cas de refus critique (par exemple si la carte a été déclarée perdue), toutes les échéances restantes sont annulées.

Si vous avez demandé l'activation 3D Secure sur votre contrat, ce mode de paiement utilise l'authentification 3D Secure uniquement sur la première échéance.

1.5.6 Paiement agrégé

Le principe de ce mode de paiement est de permettre au commerçant d'agréger plusieurs paiements et de ne faire qu'une seule et unique autorisation pour tous ces paiements. Le commerçant peut donc optimiser les paiements à faible montant.

Le commerçant paramètre le délai à partir duquel l'autorisation sera déclenché et éventuellement, le montant limite de déclenchement de l'autorisation. Pour chaque paiement effectué pour une carte bancaire donnée, le délai et le montant limite seront vérifiés. Si l'un des deux critères est atteint, une autorisation est déclenchée. Dans le cas contraire, une vérification de carte est effectuée et le paiement est agrégé aux paiements précédents.

Ce mode de paiement utilise l'authentification 3D Secure.

1.6 L'option re-crédit

Cette option ne peut être ouverte qu'après la mise en production de votre terminal. Elle vous permet de re-créditer tout ou une partie du montant d'une commande déjà payée. Le re-crédit des paiements se fait par l'intermédiaire de votre tableau de bord commerçant.

1.7 L'option Vente par Correspondance (VPC)

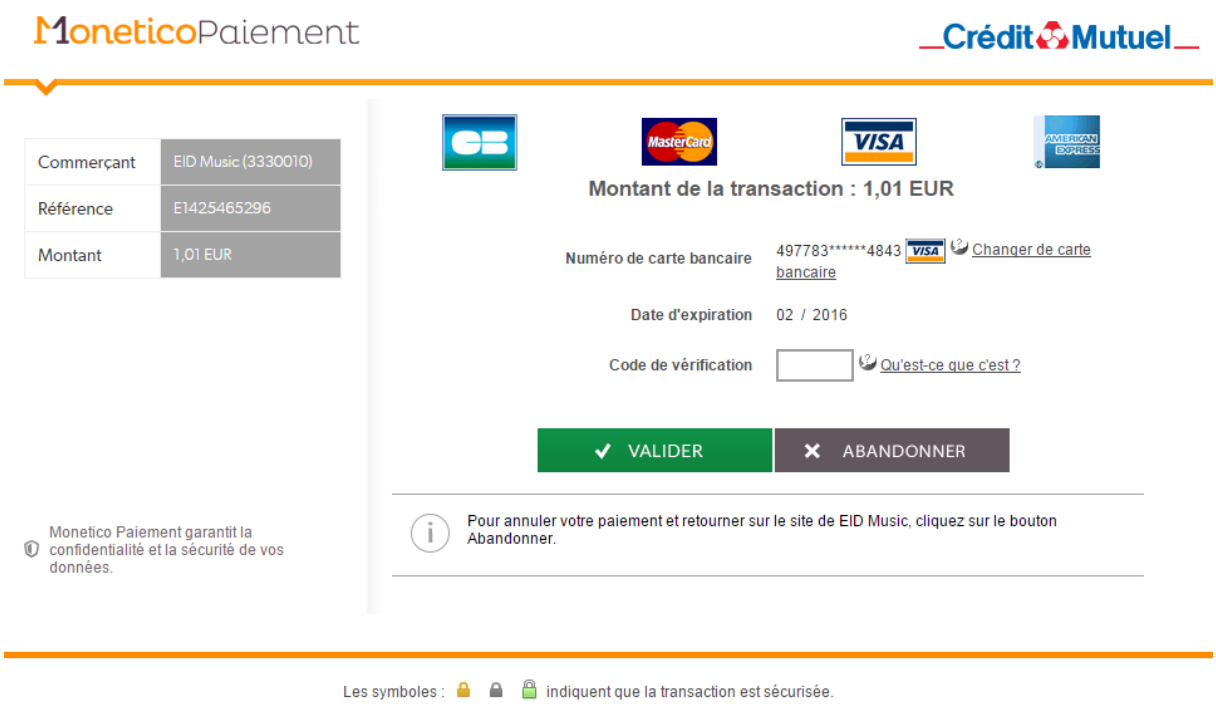
Cette option peut être ouverte immédiatement sur votre terminal. Elle vous permet de saisir vous-même le numéro de carte de votre client pour valider une commande. La VPC se fait par l'intermédiaire de votre tableau de bord commerçant. Cette option est assujettie à l'accord de votre correspondant bancaire habituel.
Un nouveau paragraphe (« Saisie d'une commande transmise par téléphone/courrier ») apparaît dans votre gestionnaire commerçant :

Figure 4 : Exemple de commande saisie en mode VPC

1.8 L'option paiement express

Cette option peut être ouverte immédiatement sur votre terminal. Elle permet de faciliter au maximum le processus de paiement pour le client. Son principe est d'associer les données bancaires du client à un alias unique que vous nous fournissez. L'authentification 3DSecure du client est obligatoire pour que la carte soit stockée.

Lors des paiements ultérieurs, le client n'aura plus qu'à saisir le code de vérification qui figure au dos de sa carte.



Cette option n'est disponible que pour les modes de paiement immédiat, différé et partiel.

1.9 Le Module Prévention Fraude

Cette fonctionnalité permet de limiter les paiements à risque par la mise en place de filtres selon plusieurs critères paramétrables (adresses IP indésirables, numéros de CB indésirables…). Ainsi, les paiements satisfaisant ces règles seront bloqués.

2. Technique et échanges

2.1. Protocole

Le schéma et le paragraphe suivants présentent la cinématique des échanges intervenant lors d'un paiement, entre l'acheteur, le serveur Web du commerçant et le serveur sécurisé de la banque.

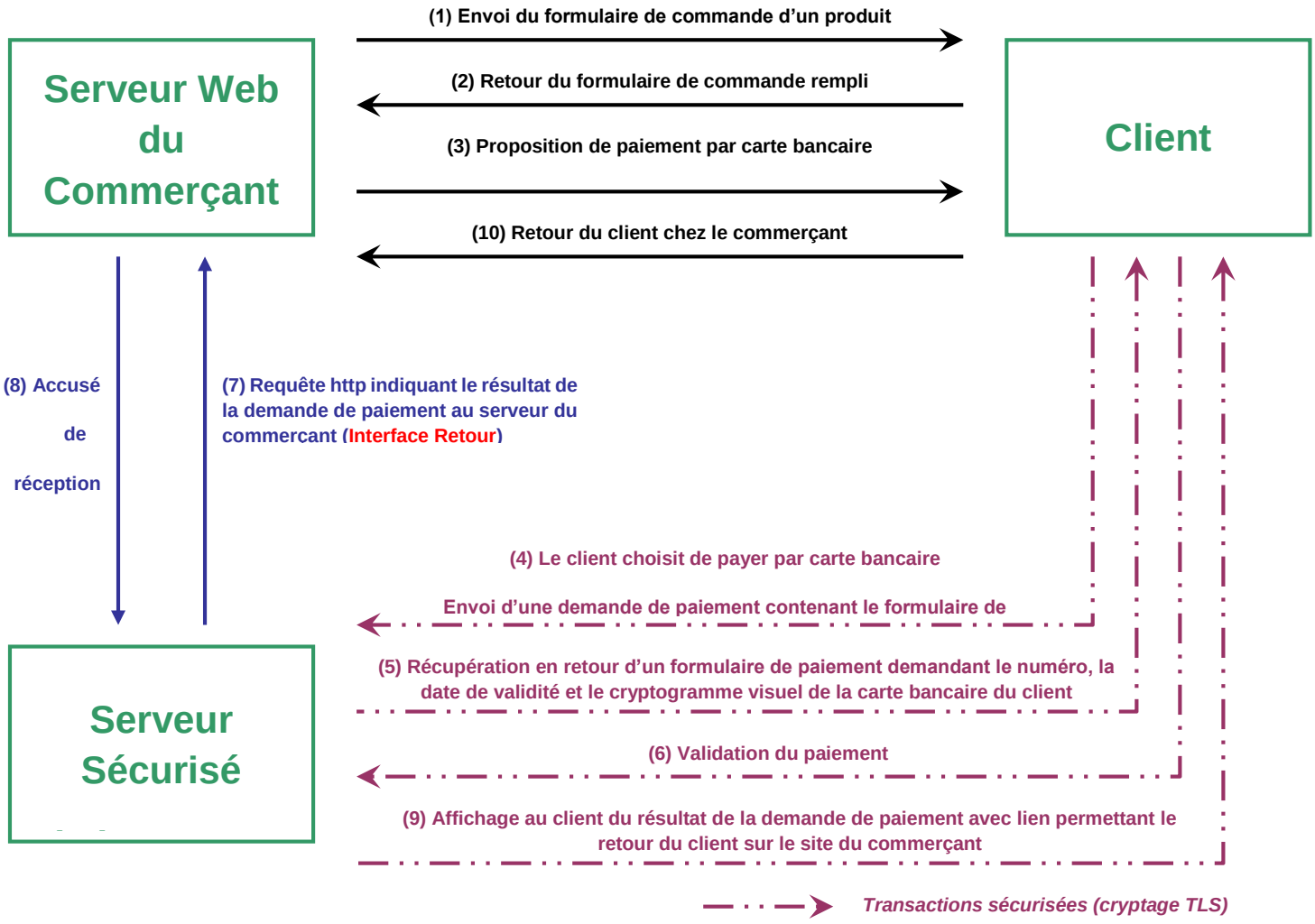


Figure 5 : déroulement d'un paiement en ligne

L'interfaçage du serveur du commerçant avec le serveur de paiement de la banque s 'effectue par l'intermédiaire de deux programmes, situés sur le serveur marchand.

Nous les appellerons ici interface « Aller » et interface « Retour » ; ils interviennent respectivement dans les phases (3) et (7).

Un paiement se passe de la façon suivante :

(1) L'acheteur parcourt le catalogue des produits et remplit son caddie virtuel

(2) Le serveur du commerçant affiche un résumé de la commande

(3) **Préparation de la phase aller du paiement : génération du formulaire de demande de paiement**

Le serveur du commerçant propose à l'acheteur un bouton « Paiement par carte bancaire ». Ce bouton va agir comme charnière entre la phase de commande et la phase de paiement : lorsque l'acheteur cliquera sur ce bouton, il sera dirigé vers le serveur de paiement sécurisé de la banque.

Ce bouton est en réalité la seule partie visible d'un formulaire HTML contenant toutes les informations relatives à la commande qu'il est nécessaire de transmettre au serveur de la banque (le montant de la commande, sa référence, le numéro du TPE virtuel du commerçant, etc.). En cliquant sur ce bouton, l'acheteur arrive sur le site de paiement sécurisé de la banque en ayant apporté avec lui ces informations.

L'interface « Aller » est chargée de générer ce formulaire HTML. Le développement de ce lien entre boutique et serveur de paiement reste sous l'entière responsabilité du marchand (ou de ses prestataires de développement/intégration).

(4) Lorsque l'acheteur clique sur le bouton « *Paiement par carte bancaire* », il arrive sur le serveur sécurisé de la banque, accompagné des informations de la commande nécessaires au paiement.

(5) Le serveur de la banque propose à l'acheteur un formulaire de saisie du numéro, de la date de validité et du cryptogramme visuel de sa carte bancaire.

(6) L'acheteur valide le paiement. La banque vérifie la validité de la carte bancaire. Différents niveaux de vérification sont effectués selon le mode de fonctionnement du TPE (mode tel que décrit plus haut).

(7) **Phase retour du paiement**

Le serveur de la banque informe directement le système informatique du commerçant du résultat de la demande de paiement en émettant une requête http(s) sur l'adresse de confirmation des paiements (en d'autres termes, **le serveur de la banque appelle l'interface « Retour »** placée sur la machine du commerçant).
Vous devez nous indiquer cette adresse URL au moment de la mise en place du système et en cas de changement (modification de nom de domaine ou de répertoire).

(8) Le système informatique du commerçant accuse réception de la confirmation du paiement.

En pratique, l'interface « Retour » est chargée de recevoir la requête de confirmation du paiement, d'en extraire les différentes informations et de répondre au serveur bancaire par un accusé de réception.
Les informations reçues par l'interface « Retour » permettent de déterminer la commande concernée, ainsi que le résultat de la demande de paiement. Cela permet au serveur du commerçant d'effectuer des traitements spécifiques :

- Vérifier que le montant et la référence correspondent au règlement d'une commande enregistrée en attente de paiement
- Mettre à jour le statut de la commande dans les bases de données
- Envoyer un courriel de confirmation au commerçant et/ou à l'acheteur
- Etc.

Attention : la commande doit être persistante dans le système commerçant (fichier, base de données) dès le début du processus et ne doit pas être détruite même après un premier avis de refus de paiement.

En effet, un refus peut être suivi d'un accord (l'interface « Retour » peut donc être appelée plusieurs fois pour une même commande), par exemple en cas d'erreur de saisie ou de plafond CB atteint ; l'acheteur peut donc vouloir utiliser une autre carte pour effectuer son paiement.

(9) Le serveur de la banque affiche à l'acheteur le résultat du paiement et propose sur cet écran un lien hypertexte lui permettant de retourner sur le site du commerçant.

Les points (8) et (9) sont des actions simultanées dans le déroulement de paiement.

(10) L'acheteur retourne, s'il le souhaite, sur le site du commerçant.

2.2. Interfaçage serveur commerçant / serveur de paiement

L'interfaçage du serveur Web du commerçant avec le serveur de paiement de la banque s'effectue par l'intermédiaire des interfaces « Aller » et « Retour », qui interviennent respectivement dans les phases *(3)* et *(7)* décrites précédemment. Ces interfaces sont placées sur la machine sur laquelle est hébergé le serveur Web du commerçant.

Euro Information ne fournit pas ces deux interfaces ; cependant une spécification et des exemples d'implémentation de la RFC2104 dans les principaux langages de script serveur (ASP, PHP, C/C++, Java, ASP/C#.NET, ASP/VB.Net, Python, Ruby) sont fournis. La plupart des environnements disposent d'une fonction de base RFC2104 (« hmac-sha1 ») ; aucun binaire n'est à installer dans ces cas de figure.

L'interface « Aller » intervient pour la génération du formulaire HTML de demande de paiement de la phase *(3)* ; pour créer ce formulaire et pour prendre en compte les aspects de sécurisation des échanges requis par notre protocole, il peut :

- soit être fait appel aux exemples Euro Information,
- soit implémenter une fonction équivalente, conforme à nos spécifications et à la RFC2104 (se référer à www.ietf.org/rfc/rfc2104.txt).

On notera que :

- La référence de la commande doit être unique. Elle doit être modifiée (incrémentation par exemple) avant chaque appel de la création du formulaire de paiement
- Le premier caractère « , » ou « . » sera considéré comme marque décimale dans le montant de la commande. Ainsi « 1.23EUR » mais aussi « 1.234,50EUR » seront donc équivalents à 1,23EUR (virgule décimale française)

L'interface « Retour » intervient dans la phase retour du paiement *(7)* ; elle a pour premier rôle de recevoir le message de confirmation du paiement émis par le serveur de la banque. Il est de la responsabilité de l'application commerçant qui reçoit ces informations, d'en faire un bon usage.

L'interface « Retour » a pour second rôle de répondre à cette requête par une confirmation ou infirmation de bonne réception du message. Elle doit pour cela :

- Soit faire appel à la fonction de calcul et de test de la valeur du sceau de certification des informations renvoyées par le serveur bancaire puis à la fonction de génération de l'accusé de réception à envoyer au serveur de la banque, présentes dans les exemples Euro Information,
- Soit implémenter des fonctions équivalentes, conformes à nos spécifications et à la RFC2104.

La nature du travail à réaliser pour la création des interfaces « Aller » et « Retour » nécessite impérativement des compétences de base en programmation et/ou script dans un langage disponible sur l'environnement du commerçant, et disposant d'une implémentation de la RFC2104.

Le développement de ces interfaces « Aller » et « Retour » et leur intégration dans le système d'information du commerçant s'effectuent sous l'entière responsabilité du commerçant ou de son prestataire 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 : paiement@cm.monetico-services.com
    - CIC : paiement@cic.monetico-services.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.

3. Installation de la solution

3.1. Etape 1 : Fourniture d'éléments techniques

Euro Information envoie à la société signataire du contrat commerçant ou à son contact technique désigné au contrat :

- les spécifications techniques d'interfaçage avec la banque
- les exemples de mise en œuvre de composants (HMAC-MD5 ou HMAC-SHA1) permettant d'authentifier les échanges avec la banque (ces composants existent dans tous les environnements, en général disponibles en standard, plus rarement assortis d'une licence particulière à laquelle le commerçant devra se conformer)

En même temps, Euro Information envoie un courriel au commerçant lui demandant les éléments permettant le paramétrage du serveur de paiement.

3.2. Etape 2 : Fourniture de la clé de sécurité du commerçant

Cette étape est déclenchée à réception par Euro Information des contrats commerçant correctement remplis et avalisés par le centre monétique de sa banque. Euro Information envoie à la société signataire du contrat commerçant :

- un identifiant et mot de passe permettant l'accès à son gestionnaire de commandes en phase de test et de production,
- un courriel invitant le commerçant à se connecter à son tableau de bord pour récupérer la clé de sécurité.

3.3. Etape 3 : Paramétrage du serveur de paiement de test

Cette étape est déclenchée à réception par Euro Information des éléments permettant le paramétrage du serveur de paiement.

Euro Information envoie au commerçant ou à son interlocuteur technique désigné au contrat, un courriel contenant la confirmation du paramétrage du serveur de paiement de test. La société dispose à ce stade de tous les éléments pour conduire et valider ses développements dans l'environnement de test.

3.4. Etape 4 : Mise en production du TPE virtuel du commerçant

Cette étape est déclenchée à réception par Euro Information d'un courriel du commerçant demandant la mise en production de son TPE virtuel; la présence de tests complets et concluants sur le serveur de paiement est indispensable.

La mise en production ne pourra se faire que si trois paiements successifs réussis au cours des 15 derniers jours ont été réalisés. Un paiement réussi est un paiement pour lequel la demande d'autorisation a été acceptée et pour lequel le retour CGI2 soit correctement traité par le commerçant.

Euro Information envoie alors au commerçant un courriel de confirmation de l'ouverture en production de son TPE virtuel, et rappelant qu'il dispose d'un identifiant et d'une adresse dédiée au suivi de ses paiements.

3.5. URLs des serveurs de paiement

3.5.1. En Test

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

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

3.5.2. 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/paiement.cgi

Nous attirons votre attention sur le fait que les formulaires de paiement adressés au serveur de production seront des paiements réels.

3.6. URLs du tableau de bord commerçant

3.6.1. En Test

Le tableau de bord commerçant de l'environnement de test est disponible à l'adresse suivante :

- https://www.monetico-services.com/fr/test/identification/login.cgi

3.6.2. En Production

Vous pouvez consulter les paiements opérés sur votre TPE via le tableau de bord commerçant disponible à l'adresse suivante :

- https://www.monetico-services.com/fr/identification/login.cgi