

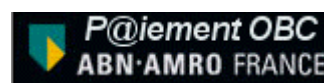
CyberMUT P@iement



P@iement CIC



P@iement OBC



***SERVICE SECURISE DE
PAIEMENT INTERNET PAR CARTE BANCAIRE
(Sécurisé par le protocole SSL)***

Présentation Générale

(Document 1/2)



**EURO
INFORMATION**

TABLE DES MATIERES

Présentation Générale	1
1. PRESENTATION DU SERVICE DE PAIEMENT PAR CARTE BANCAIRE SUR INTERNET, SECURISE PAR SSL.	3
1.1. PRINCIPE.	4
1.2. CARACTERISTIQUES PRINCIPALES DU SYSTEME DE PAIEMENT.	4
1.3. DESCRIPTION DE LA PHASE PAIEMENT	6
1.4. SUIVI DES PAIEMENTS PAR LE COMMERÇANT	8
1.5. L'OPTION RE-CREDIT	16
1.6. PROTOCOLE.	17
1.7. INTERFAÇAGE SERVEUR COMMERÇANT / SERVEUR DE PAIEMENT.	20
2. ETAPES DE L'INSTALLATION	21
2.1. ÉTAPE 1 : FOURNITURE DES ELEMENTS LOGICIELS.	21
2.2. ÉTAPE 2 : FOURNITURE DE LA CLE DE SECURITE DU COMMERÇANT.	21
2.3. ÉTAPE 3 : PARAMETRAGE DU SERVEUR DE PAIEMENT DE TEST.	22
2.4. ÉTAPE 4 : MISE EN PRODUCTION DU TPE VIRTUEL DU COMMERÇANT.	22

1. Présentation du service de paiement par carte bancaire sur Internet, sécurisé par SSL.

Le but du service de paiement par carte bancaire sur Internet, sécurisé par SSL, est de permettre aux commerçants de vendre leurs produits ou services sur Internet, de façon sécurisée, en mode " vente à distance " (VAD). Ce service est opérationnel depuis 1996.

Ce service permet de décharger le site du commerçant de toute la phase de paiement. La phase de paiement a lieu directement sur le serveur de paiement sécurisé de la banque.

La réalisation du site commerçant et son hébergement ne sont pas couverts par le service de paiement sécurisé. Vous pouvez contacter votre correspondant commercial régional pour connaître les offres de boutique packagées associées à notre service de paiement sécurisé.

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 oeuvre 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 et date de validité de la carte bancaire) assurée par chiffrement SSL,
- 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.

1.1. Principe.

Le commerçant présente un catalogue de services ou de produits sur un serveur web. Sur ce serveur web, l'acheteur consulte le catalogue, passe sa commande puis choisit son moyen de paiement. Dans le cas d'un paiement par carte bancaire, il est dirigé vers le service de paiement par carte bancaire de la banque.

Pendant toute la phase de paiement, l'acheteur dialogue directement avec le serveur de paiement sécurisé de la banque. Les échanges se passent en mode sécurisé garantissant la confidentialité des informations fournies par l'acheteur (numéro et date de validité de la carte bancaire).

Après validation de la requête par l'acheteur, la banque se charge d'effectuer :

- la demande d'autorisation du paiement (contrôle de la structure du numéro de carte bancaire, contrôle sur le fichier des cartes volées / en opposition, interrogation de la banque de l'acheteur par le réseau inter-bancaire pour obtention de l'autorisation de paiement),
- l'envoi d'un message de confirmation précisant le résultat du paiement vers le système informatique du commerçant,
- la mise en recouvrement du paiement.

1.2. Caractéristiques principales du système de paiement.

➤ Cartes bancaires acceptées :

- Cartes bancaires nationales françaises
- Cartes EuroCard / MasterCard internationales
- Cartes Visa internationales

Sous réserve de conclusion, entre l'acheteur et l'organisme financier concerné :

- American Express (Nov 2001)

➤ Devises acceptées :

- Franc français (**FRF**) (*jusqu'au 31/12/2001*)
- Euro (**EUR**)
- Devises IN

Sous réserve de conclusion, entre l'acheteur et sa banque, des contrats de gestion de devises correspondants

- Dollar (**USD**)
- Franc suisse (**CHF**)
- Livre sterling (**GBP**)

➤ **Pages du serveur de paiement** disponibles en :

- Français
- Anglais
- Allemand
- Italien
- Espagnol

➤ **Logo du commerçant :**

Personnalisation des pages de paiement possible avec le logo du commerçant. (GIF 120*120 maxi). Nous fournir l'URL de l'image GIF située sur le serveur du commerçant.

➤ **Le Paiement :**

- Affichage permanent des informations commerçant (nom, identifiant, logo, référence de la transaction)
- Affichage en fin de phase de paiement d'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)
- Envoi d'un mail d'alerte en cas de problème de retour d'information sur le serveur commerçant
- Option permettant d'envoyer un mail de confirmation de paiement directement au commerçant (cette option ne peut se substituer au message de confirmation en ligne existant dans le protocole) ;
- Option payante permettant d'envoyer un fax de confirmation de paiement directement au commerçant

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.

Solution CyberMUT P@iement :

P@iement Sécurisé
par Carte Bancaire



Montant de la transaction : 1 FRF



Numéro de carte bancaire

Date d'expiration (Mois / Année) /

3 derniers chiffres du numéro imprimé au dos (Cryptogramme Visuel)

Le panneau de signature, au dos de votre carte, ne comporte pas de numéro

... ou comporte un numéro, saisissez les 3 derniers chiffres

Cliquer sur la carte pour obtenir des informations détaillées

***Votre transaction est sécurisée par CyberMUT P@iement.
Votre paiement sera réalisé en toute sécurité.***

[Annuler et retourner à la société La boutique du CD](#)

La Boutique du CD

Identifiant Commerçant :
0900157

Référence Transaction :
4578

L'acheteur entre son numéro de carte bancaire, la date de validité, et éventuellement le cryptogramme visuel situé au dos de sa carte. Ensuite, il clique sur le bouton " valider ".

Solution P@iement CIC :



La boutique du CD
Identifiant Commerçant :
0900157
Référence Transaction :
4578



**Paiement sécurisé sur Internet**

Montant de la transaction : 1 FRF

Numéro de carte bancaire

Date d'expiration (Mois / Année) /

3 derniers chiffres du numéro imprimé au dos (Cryptogramme Visuel)

Le panneau de signature, au dos de votre carte, ne comporte pas de numéro

... ou comporte un numéro, saisissez les 3 derniers chiffres

Cliquer sur la carte pour obtenir des informations détaillées

***Votre transaction est sécurisée par P@iement CIC.
Votre paiement sera réalisé en toute sécurité.***

[Annuler et retourner à la société La boutique du CD](#)

A l'issue du paiement, le site sécurisé de la banque affiche une page d'information avec un lien (dont le texte est personnalisable), qui permet à l'acheteur de retourner sur le site du commerçant.

Solution P@iement OBC :

 <p>ODIER BUNGENER COURVOISIER</p>		<p>P@iement sécurisé par cartes bancaires</p>   	
 <p>La boutique du CD</p>		<p>Demande d'autorisation carte en cours ...</p> <p>Votre carte bancaire a été acceptée. La boutique du CD en a été informé.</p>	
<p>Identifiant Commerçant : 0900157</p>		<p>Montant de la transaction : 1 FRF Date de la transaction : 2001-10-16 15:48:35 (UTC/GMT) Numéro de la carte : 513283#####26</p>	
<p>Référence Transaction : 4578</p>		<p>Numéro d'autorisation : 554130 Numéro de terminal : 0900157</p>	
<p>Cliquez ici pour revenir à la société La boutique du CD</p>			

1.4. Suivi des paiements par le commerçant

Une base de données contient, pour chaque commerçant, la liste des paiements effectués lors des 4 derniers mois. Le commerçant consulte cette base de données sur le serveur web de la banque. Ce service est appelé le "gestionnaire commerçant" ou le "tableau de bord commerçant".



Page d'accueil

Solution **CyberMUT P@iement** : <https://www.creditmutuel.fr/telepaiement>



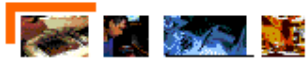
The screenshot shows a merchant dashboard for CyberMUT P@iement. At the top, there is a banner with the text "P@iement Sécurisé par Carte Bancaire" and logos for Euro-Information, Crédit Mutuel, and various payment cards (Eurocard, MasterCard, VISA). The main content area is divided into several sections:

- Tableau de bord commerçant**: A summary section stating "Aujourd'hui, aucun paiement mis en recouvrement." and "5 paiements en attente de votre traitement."
- Historique des paiements effectués**: A list of links for "Présentation par date de commande" and "Présentation par date de mise en recouvrement".
- Historique des recredits effectués**: A list of links for "Présentation par date de recrédit".
- Historique des paiements en attente**: A list of links for "Liste des paiements différés en attente de traitement" and "Recherche d'un paiement différé en attente de traitement". Below this is a search form with the text "Saisir une référence :", an input field, and a "Recherche" button.
- Historique des paiements partiels en attente de traitement**: A list of links for "Liste des paiements partiels en attente de traitement" and "Recherche d'un paiement partiel en attente de traitement". Below this is another search form with the text "Saisir une référence :", an input field, and a "Recherche" button.
- Gestion de votre identifiant**: A list of links for "Changez votre mot de passe".

On the left side of the dashboard, there is a logo for Euro-Information 7000000.

Après identification...

Consultation de la liste de vos commandes :


CIC
Banques

Euro-Information
7000000*Paiement sécurisé sur Internet**Historique des paiements effectués pour les 120 derniers jours*

Cliquez sur une date pour obtenir la liste des paiements
de la journée correspondante.

Date de commande	Nb. de paiements
01/10/2001	1
26/09/2001	1
12/09/2001	1
06/09/2001	6
05/09/2001	1
04/09/2001	2
08/08/2001	1
23/07/2001	1
20/07/2001	1
19/07/2001	1
09/07/2001	2
05/07/2001	1
22/06/2001	1

[Précédent](#)

Présentation des commandes par date de mise en recouvrement, il est possible de télécharger un fichier XML contenant un récapitulatif des commandes payées sur un journée :



P@iement Sécurisé
par Carte Bancaire

Crédit Mutuel
La Banquassurance

MasterCard VISA

Historique des paiements effectués pour les 120 derniers jours

Cliquez sur une date pour obtenir la liste des paiements de la journée correspondante.

Nouveauté: clic droit sur le lien XML pour télécharger les paiements du jour.

Date de demande de mise en recouvrement	Nb. de paiements	Téléchargement
03/10/2001	1	XML
01/10/2001	1	XML
12/09/2001	1	XML
06/09/2001	5	XML
05/09/2001	1	XML
04/09/2001	2	XML
08/08/2001	1	XML
24/07/2001	1	XML
20/07/2001	1	XML
19/07/2001	1	XML
09/07/2001	3	XML

Précédent

Euro-Information
7000000

Ouvrir
Ouvrir dans une nouvelle fenêtre
Enregistrer la cible sous...
Imprimer la cible
Copier
Copier
Copier le raccourci
Clic
Ajouter aux Favoris...
Propriétés

Trois modes de fonctionnement (exclusifs l'un de l'autre) sont offerts :

- 1 Paiement immédiat
- 2 Paiement différé
- 3 Autorisation différée (Paiement partiel)

Un TPE fonctionne dans un seul mode (inscrit au contrat).

➤ **Paiement immédiat :**

La demande d'autorisation du paiement est effectuée "on line" à la commande.
La mise en recouvrement est faite immédiatement.

➤ **Paiement différé**

La demande d'autorisation du paiement est effectuée "on line" à la commande.
La mise en recouvrement est faite en back-office.

Lorsque le commerçant a opté pour le paiement différé, il consulte, pendant la période de différé, la liste de ses paiements en attente sur le serveur web de la banque, et il peut alors manuellement valider ou annuler ces paiements, ou les laisser en attente.

Le commerçant peut opter pour une validation automatique ou un rejet automatique à la fin de la période de différé.

La période de différé de recouvrement est fixée dans le contrat, avec un maximum de 7 jours ouvrés (le risque de mise en opposition de la carte entre l'autorisation et le recouvrement augmente avec la durée du différé).

Solution **CyberMUT P@iement** : <https://www.creditmutuel.fr/telepaiement>

Exemple avec l'option " **annulation automatique** " en fin de période :

P@iement Sécurisé
par Carte Bancaire







Euro-Information
7000000

Historique de la commande

Les paiements suivants ont été autorisés par la banque. Durant la période de différé, ces paiements restent en **attente d'un traitement manuel de votre part**:

- Valider** : pour mettre le paiement en recouvrement.
- Annuler** : pour supprimer le paiement.


Les paiements ni validés ni annulés seront **automatiquement annulés à la date indiquée**. Vous pouvez obtenir le détail d'une demande de paiement en cliquant sur sa référence.

Date	Référence	Montant de la commande	Valider	Laisser	Annuler	Date d'annulation automatique
27/09/2001	485424220562	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	08/10/2001
06/09/2001	421932399273	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	17/09/2001
05/09/2001	226055324078	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	14/09/2001
04/09/2001	914806544780	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	13/09/2001

Références de couleur rouge : votre serveur commerçant n'a pas (ou mal) répondu à la confirmation d'enregistrement des informations de paiement émise par notre serveur de paiement au moment de l'achat.



Exemple avec l'option " **validation automatique** " en fin de période :

ABN-AMRO FRANCE **BANQUE OBC** 

BANQUE OBC - ODIER BUNGENER COURVOISIER

Paiement sécurisé sur Internet

Historique de la commande


Les paiements suivants ont été autorisés par la banque. Durant la période de différé, ces paiements restent en **attente d'un traitement manuel de votre part**:

- **Valider** : pour mettre le paiement en recouvrement.
- **Annuler** : pour supprimer le paiement.

Les paiements ni validés ni annulés seront **automatiquement validés à la date indiquée**. Vous pouvez obtenir le détail d'une demande de paiement en cliquant sur sa référence.

Date	Référence	Montant de la commande	Valider	Laisser	Annuler	Date de validation automatique
27/09/2001	485424220562	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	08/10/2001
06/09/2001	421932399273	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	17/09/2001
05/09/2001	226055324078	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	14/09/2001
04/09/2001	914806544780	1 FRF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	13/09/2001

Références de couleur rouge : votre serveur commerçant n'a pas (ou mal) répondu à la confirmation d'enregistrement des informations de paiement émise par notre serveur de paiement au moment de l'achat.




Euro-Information
7000000


➤ Autorisation différée (Paiement partiel)

La demande d'autorisation du paiement est effectuée en back-office lors de la validation du paiement par le commerçant.

Si le commerçant a opté pour le mode autorisation différée, il peut également consulter la liste des paiements en attente sur le serveur web de la banque : il peut alors manuellement valider totalement ou partiellement (en une ou plusieurs fois) ou annuler tout ou partie de ces paiements, ou alors les laisser en suspens pour une annulation automatique en fin de période de différé.

Solution P@iement CIC : <https://ssl.paiement.cic-banques.fr>





 Euro-Information
7000000

Paiement sécurisé sur Internet

Historique de la commande

Les demandes de paiement suivantes ont été effectuées sur votre TPE. Durant la période de différé, ces demandes de paiement sont en **attente d'un traitement manuel de votre part** :

- **Validation Totale (VT)** : pour mettre la totalité du montant en recouvrement.
- **Validation Partielle (VP)** : pour mettre une partie du montant en recouvrement.
- **Annulation** : pour supprimer le paiement.

Une autorisation de paiement est demandée au moment de votre validation (totale ou partielle) et tout paiement autorisé sera mis en recouvrement.
Vous pouvez obtenir le détail d'une demande de paiement en cliquant sur sa référence.


Date	Référence	Montant de la commande	Montant restant à recouvrer	Montant à recouvrer	Date d'annulation automatique
04/09/2001	222222	1 FRF	1 FRF	<input type="radio"/> VT <input type="radio"/> VP <input style="width: 50px; height: 20px;" type="text"/> <input checked="" type="radio"/> Laisser <input type="radio"/> Annuler	13/09/2001

Références de couleur rouge : votre serveur commerçant n'a pas (ou mal) répondu à la confirmation d'enregistrement des informations de paiement émise par notre serveur de paiement au moment de l'achat.

1.5. 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 partie du montant d'une commande déjà payée. Le re-crédit des paiements se fait par l'intermédiaire de votre gestionnaire commerçant.

Une nouvelle colonne ("Montant re-crédité") apparaît dans votre gestionnaire commerçant:



Euro-Information
7000000

Liste des **paiements effectués** sur votre TPE le **26/09/2001**.

Cliquez sur une référence de commande pour obtenir le détail.

Heure	Référence	Montant TTC	Autorisation	Montant re-crédité
15:53:23	83	464.53 EUR	459463	0 EUR

Références de couleur rouge : votre serveur commerçant n'a pas (ou mal) répondu à la confirmation d'enregistrement des informations de paiement émise par notre serveur de paiement au moment de l'achat.

Vous pouvez accéder à la fonction de re-crédit en cliquant sur la référence d'une commande payée. La page de détail des commandes contient un tableau intitulé "**Recouvrement(s)**" contenant le montant du re-crédit possible ainsi qu'un lien ("[cliquer ici](#)") pour effectuer un re-crédit:



Euro-Information
7000000

Détail de la commande

Détail	
Paiement par carte effectué le	26/09/2001 à 15:53:23
Référence de la commande	83
Montant	464.53 EUR
Type de carte utilisée	  

Recouvrement(s)					
Recouvré le	Numéro d'autorisation	Référence d'archivage	Montant	Re-crédit possible	Re-crédit
03/10/2001	459463	83	464.53 EUR	464.53 EUR	cliquer ici

Re-crédit

Aucun re-crédit n'a été effectué pour cette commande.

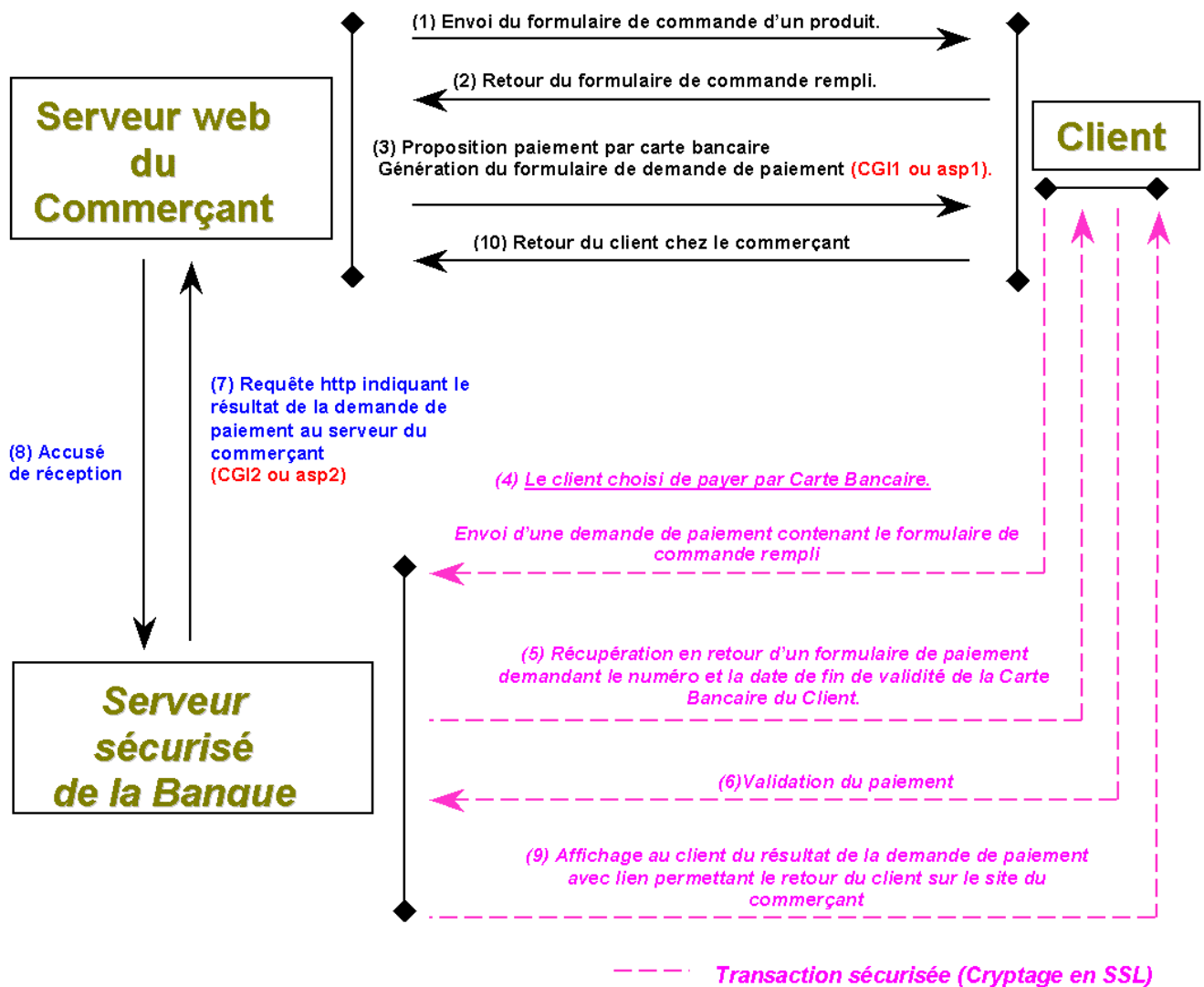
Descriptif

2 BIC Bleu (par 10), 7 Calvados



1.6. 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.



L'interfaçage du serveur du commerçant avec le serveur de paiement de la banque s'effectue par l'intermédiaire de 2 programmes CGI : **CGI1 (ou asp1)** et **CGI2 (ou asp2)**, qui 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 (bon de 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.

Un certain nombre d'informations relatives à la commande sont nécessaires pour le traitement du paiement. Il s'agit des informations telles que le *montant de la commande*, sa *référence*, le *numéro du TPE virtuel* du commerçant, etc. **Ces informations doivent être associées au bouton "*Paiement par carte bancaire*" afin d'être fournies au serveur de paiement lorsque l'acheteur arrive à la banque.**

En pratique, ces informations sont placées **en champs cachés** (hidden) dans un formulaire HTML, dont la seule partie visible pour l'acheteur est le bouton de validation (submit) intitulé "*Paiement par carte bancaire*".

Le CGI1 (ou asp1) est chargé de générer ce formulaire HTML : pour cela il doit impérativement faire appel à la fonction *CreerFormulaireCM ()* présente dans la librairie fournie (prise en compte des aspects de sécurisation des échanges).

La référence de la commande doit être unique. Elle doit être modifiée (incrémentation par exemple) avant chaque appel de la fonction "créerformulaire".

Les "," et "." sont considérés comme décimale dans le montant de la commande. (par exemple le montant 1.234,50EUR sera considéré comme 1,23EUR par le système)

- (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 et de la date de validité de sa carte bancaire.
- (6) L'acheteur valide le paiement. La banque vérifie la validité de la carte bancaire.

(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 pratique, le serveur de la banque émet une requête HTTP contenant le résultat de la demande de paiement sur l'**URL de confirmation des paiements : cette URL correspond à l'URL du CGI2** (ou asp2) (URL que vous devez nous indiquer au moment de la mise en place du système) placé sur la machine du commerçant.

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

En pratique, le CGI2 est chargé de recevoir la requête de confirmation du paiement, d'en extraire les différentes informations, dont le résultat du paiement, et d'y répondre par un petit message d'accusé de réception : pour cela il doit impérativement faire appel à la fonction *TestMAC ()* (prise en compte des aspects de sécurisation des échanges) puis à la fonction *CreerReponseCM ()* (génération du message d'accusé de réception à répondre au serveur de la banque), présentes dans la librairie fournie.

Les informations reçues par le CGI permettent de déterminer la commande concernée, ainsi que le résultat de la demande de paiement. Cela permet au serveur du commerçant, d'effectuer certains traitements spécifiques:

- Vérifier que le montant correspond au montant de la commande enregistrée.
- Mise à jour base de données
- Envoi d'un mail de confirmation au commerçant
- Envoi d'un mail de confirmation à l'acheteur
- Etc...

Une commande doit être persistante et ne doit pas être détruite dès le premier accusé de refus de paiement. (cas de mauvaise saisie de la carte)

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

1.7. 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 de **deux petits programmes de type CGI ou ASP : CGI1 et CGI2 (ASP1 et ASP2)**, qui interviennent respectivement dans les phases **(3)** et **(7)** décrites précédemment. Ces CGIs (ou ASPs) sont placés sur la machine sur laquelle est hébergé le serveur web du commerçant.

Euro-Information ne fournit pas directement ces deux CGIs (ou ASPs) d'interfaçage du serveur web du commerçant avec le serveur de la banque, **mais des éléments logiciels se présentant sous la forme d'une boîte à outils** (bibliothèque de fonctions ou DLL) qu'il faut impérativement utiliser pour créer ces CGIs ou ASPs.

Euro-Information fournit des exemples de CGI dans les langages suivants: C, Perl, PHP, Java, ASP, et Cold Fusion. Le petit travail de programmation relatif au développement de ces deux CGIs (ou ASPs) incombe à la société qui souhaite mettre en œuvre le paiement sécurisé sur sa machine.

Le **programme CGI1 (ou ASP1)** intervient simplement pour la **génération du formulaire HTML de demande de paiement** de la phase **(3)**. Il est basé sur l'utilisation d'une fonctionnalité présente dans les éléments logiciels fournis par Euro-Information, qui permet de créer le formulaire de demande de paiement contenant les informations de contexte de la commande.

Pour des raisons de sécurisation des échanges, le formulaire de demande de paiement doit impérativement être généré en utilisant cette fonctionnalité.

Le **programme CGI2 (ou ASP2)** intervient dans la **phase retour du paiement (7)**. En effet, le serveur de la banque **informe directement le système informatique du commerçant du résultat de la demande de paiement**.

Le CGI2 (ou ASP2) a pour rôle de **recevoir le message de confirmation du paiement** émis par le serveur de la banque.

Placé sur la machine du commerçant, il reçoit une requête HTTP émise par le serveur de la banque. Les informations communiquées au CGI2 (ou ASP2) permettent de déterminer la commande concernée, ainsi que le résultat de la demande de paiement. Il est de la responsabilité de l'application commerçant qui reçoit ces informations par l'intermédiaire du CGI2, d'en faire un bon usage.

Pour des raisons de sécurisation des échanges, les informations reçues par le CGI2 (ou ASP2) doivent être contrôlées à l'aide d'une fonctionnalité présente dans les éléments logiciels fournis par Euro-Information.

Le CGI2 (ou APS2) offre également la possibilité au serveur du commerçant, d'effectuer certains traitements spécifiques (mise à jour d'une base de données, envoi d'un mail de confirmation au commerçant, envoi d'un mail de confirmation à l'acheteur, etc.).

La nature du travail à réaliser pour la création des deux programmes CGI1 et CGI2 nécessite impérativement des compétences en programmation.

2. Etapes de l'installation

2.1. Etape 1 : Fourniture des éléments logiciels.

Cette étape est déclenchée à réception par Euro Information du contrat de licence correctement rempli. Euro Information envoie à la société signataire du contrat de licence un mail contenant :

- Les éléments logiciels relatifs au système d'exploitation déclaré sur le contrat et la documentation associée ;
- Un identifiant et mot de passe permettant l'accès au serveur de paiement de test ;
- Un identifiant et mot de passe au commerçant permettant l'accès à son gestionnaire de commandes en phase de production.
- Une demande de renseignements techniques indispensables pour la poursuite de l'installation. La société doit fournir par retour de mail les informations suivantes :
 - Le nom exact de la machine sur laquelle seront installés les éléments logiciels. Ce nom est déterminé à l'aide du petit utilitaire présent dans les éléments fournis (programme "host") ;
 - Les éléments permettant le paramétrage du serveur de paiement.

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

Cette étape est déclenchée à réception par Euro Information :

- Du nom exact de la machine sur laquelle seront installés les éléments logiciels
- Eventuellement, des contrats du commerçant correctement remplis.

Euro Information envoie à la société titulaire de la licence un mail contenant la clé de sécurité du commerçant : cette clé est utilisable uniquement sur la machine pour laquelle la licence a été achetée.

Si aucun contrat commerçant n'est encore rattaché au contrat de licence, une clé de sécurité de test est fournie à la société titulaire de la licence pour que celle-ci puisse commencer à développer la solution.

2.3. 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 (informations demandées dans le mail de l'étape 1). Euro Information envoie à la société titulaire de la licence un mail 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.

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

Cette étape est déclenchée à réception par Euro Information :

- D'un mail de la société titulaire de la licence indiquant que ses développements relatifs au site du commerçant sont terminés et valides (présence de tests concluant sur le serveur de paiement de test indispensables) ;
- D'un mail du commerçant demandant la mise en production de son TPE virtuel.

Euro Information envoie :

- A la société titulaire de la licence : un mail de confirmation de la mise en production du TPE virtuel du commerçant, contenant l'adresse du serveur de paiement de production ;
- Au commerçant : un mail de confirmation de l'ouverture en production de son TPE virtuel, contenant l'identifiant permettant l'accès au gestionnaire commerçant.