ClicToPay.com

ClicToPay (2016)

Plateforme de paiement électronique

Présentation Clictopay

Version 1.0

I. SmartVista ClicToPay system

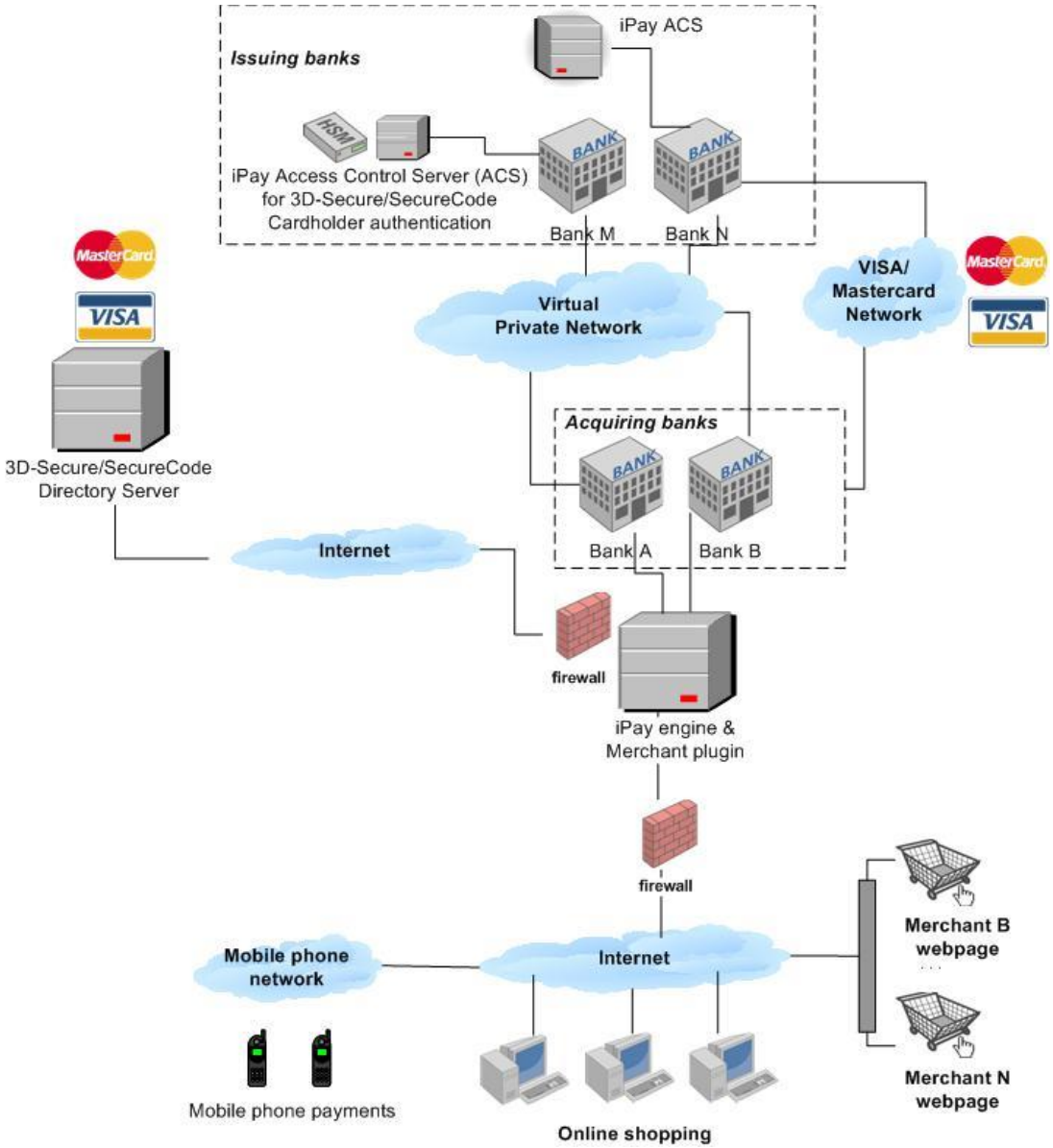
ClicToPay, est un système qui permet l'acceptation des cartes de paiement électronique, par les sites marchands, et qui utilise des technologies et normes modernes pour les paiements sur Internet.

Le système est destiné aux commerçants qui commercialisent leurs produits et services sur Internet. Le système ClicToPay est certifié par ***Visa*** et ***MasterCard*** pour l'acquisition des transactions de paiement électronique via Internet.

Du coté des porteurs des cartes bancaires, ClicToPay prend en charge les protocoles de sécurisation des paiements les plus courants à savoir « ***Verified by Visa*** » de Visa et « ***SecureCode*** » de MasterCard, qui sont des protocoles de paiement avec authentification supplémentaire du porteur de la carte, dans ce cas ce dernier doit être inscrit dans un système sécurisé.

Clictopay est doté d'un système sophistiqué de gestion des règles anti-fraude basé sur le filtrage de transaction, flexible en fonction des paramètres du paiement de commandes du marchand. Les opérateurs marchands et les utilisateurs autorisés peuvent définir des critères de détection de la fraude avec estimation du facteur de probabilité de fraude pour une transaction donnée. Le strict respect des exigences du réseau des paiements internationaux comme le programme de sécurité de l'information du titulaire de Visa (CISP), qui garantit également une sécurité supplémentaire de la solution.

Le schéma logique ClicToPay est présenté ci-dessous :



En dehors de l'ACS et MPI, BPC propose une gamme de produits e-commerce supplémentaires :

- Passerelle de paiement – environnement de base pour l'acquisition de commerce électronique. C'est une composante minimale nécessaire pour activer votre e-commerçant d'accepter les e-paiements.
- Portail marchand – solution pour les e-commerçants permettant le suivi de commande, carte stop listing, rapports et d'autres fonctionnalités.
- Prévention de la fraude électronique – solution basée sur des règles qui vise à atténuer les risques pour les acquéreurs de commerce électronique.

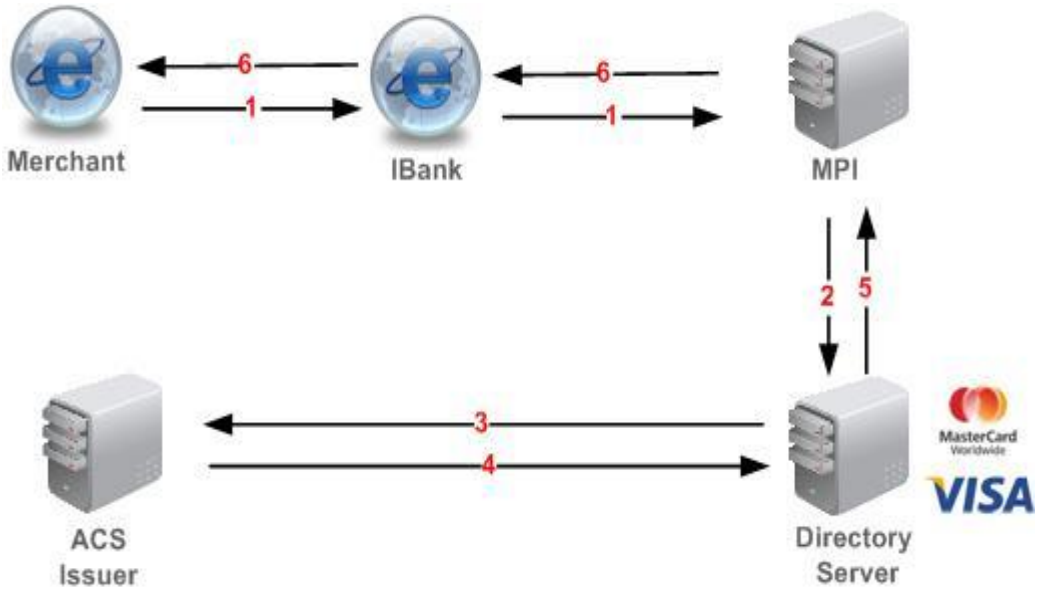
II. ClicToPay acquéreur

Le mécanisme de traitement des transactions se compose de deux parties principales :

1) Vérification de l'inscription de la carte à la technologie 3D-Secure

2) Autorisation de transaction

Le diagramme logique de la première étape est présenté ci-dessous :



Étape 1. Titulaire de la carte décide d'utiliser sa carte en plastique pour la transaction sur Internet et renseigne les paramètres d'opération sur le site Internet du marchand.

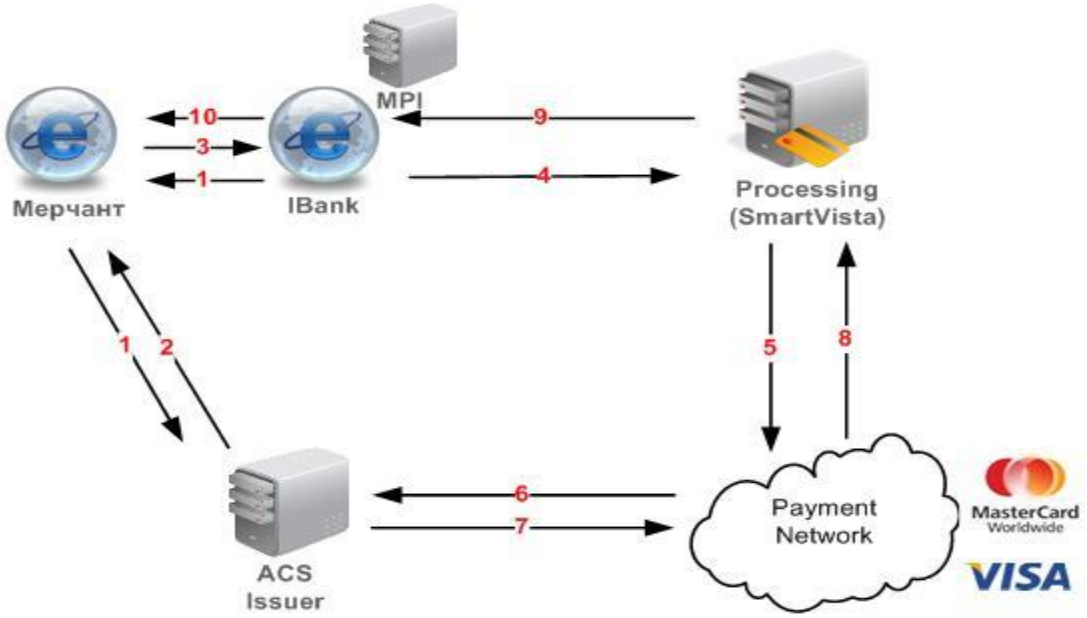
Étape 2. Pour vérifier si la carte est impliquée au technologie 3-d Secure le marchand envoie une requête au serveur annuaire (Directory server). « Merchant plug-in » est un logiciel utilisé pour la connexion avec l'annuaire (DS). Ce logiciel assure l'authentification et le chiffrement des données transférées entre le commerçant et le serveur annuaire.

Étape 3. Si la banque émettrice est impliquée dans la technologie 3D Secure l'annuaire vérifie si cette carte particulière est impliquée dans la technologie 3D Secure ou non. Ce dernier se connecte au serveur ACS de banque de l'émetteur et envoie une requête avec le numéro de carte.

Étape 4. L'ACS vérifie si la carte est impliquée dans la technologie 3D Secure en envoyant la requête HTTP GET au serveur Internet bancaire de la Banque de l'émetteur. ACS envoie la réponse à l'annuaire.

Étapes 5 et 6. Marchand reçoit cette réponse de l'annuaire. Si la Banque émetteur et la carte sont impliqués dans la technologie 3D Secure, la réponse contient le lien vers le serveur ACS de la Banque émettrice.

Le diagramme logique de la deuxième étape est illustré ci-dessous :



Étapes 1. Le serveur du marchand redirige le navigateur Internet du détenteur à l'ACS de la Banque de l'émetteur. Tout en étant authentifié le détenteur de la carte voit l'URL de la page du serveur ACS dans la barre d'adresse.

Étape 2. Le titulaire de la carte passe son login et mot de passe du système d'opérations bancaires sur Internet sur la page de l'ACS. L'ACS envoie la demande d'authentification au serveur de la Banque de l'émetteur. Dans le cas d'une authentification réussie la valeur CAVV/AAV (TCCP) doit être généré.

Étape 3. Le marchand envoie une réponse à l'émetteur avec la valeur CAVV/AAV au serveur la banque internet (I-BANK) du système bancaire.

Étape 4. Le serveur bancaire internet analyse et vérifie la réponse de l'émetteur avec l'aide de MPI. Si OK, le système bancaire internet envoie la demande d'autorisation à un système de traitement. Le message d'autorisation contient la valeur CAVV/AAV.

Étapes 5-6-7-8. Les banques acquéreur traite la transaction par le biais de réseau de paiement de manière standard. Au cours de l'autorisation de la transaction, l'émetteur vérifie la valeur CAVV/AAV.

Étape 9. Le système de traitement répond au système bancaire internet.

Étape 10. Le système bancaire internet répond au marchand.

III. Clictopay émetteur

Clictopay émetteur une partie de solution – le serveur ACS stipule ce qui suit :

- Téléchargement de plages de numéros de carte participant à la technologie 3D-Secure, en réponse à la demande du serveur d'annuaire ;
- Vérification du numéro de carte impliqué dans la technologie 3D-Secure à la demande du serveur d'annuaire ;
- Demandes d'authentification du titulaire de la carte et vérification du code entré sur le serveur ACS ;
- Envoi d'une demande pour la génération de CAVV/CAVV/AAV au système SVFE et le transfert de cette valeur au serveur du commerçant.

Le diagramme logique de ClicToPay émetteur (ACS) est exposé ci-dessous :