Complément au projet S7
« Simulateur de transactions par carte bancaire »

Ce document donne des explications sur le projet « simulateur de transactions par carte bancaire ». C'est un guide général. Vous êtes libres d'adapter et de modifier des choses à condition de rester relativement réaliste. Vous pouvez faire un programme « classique », des programmes fonctionnant en réseau, une application web… A vous de choisir.

1 Aperçu général

1.1 Le principe du paiement par carte bancaire

Le paiement par carte bancaire met en relation plusieurs acteurs :
– le client (le ***porteur***) qui souhaite régler un achat avec la carte bancaire qu'il possède et qui lui a été fournie par sa banque;
– le commerçant (l'***accepteur***) qui est équipé d'un terminal de paiement fourni par sa propre banque;
– la banque X du commerçant (l'***acquéreur***) à laquelle est connecté le terminal de paiement ;
– la banque Y du client (l'***émetteur***) qui va dire si la transaction est autorisée (donc si le compte de son client est suffisamment provisionné ou non, etc.).

Le terminal du commerçant est relié à la banque X grâce à une simple ligne téléphonique. La banque X est connectée à toutes les autres banques installées en France, et notamment à la banque Y, grâce à un réseau dédié : le ***réseau interbancaire***.

Supposons maintenant que le client C se rend chez son revendeur de matériels préféré pour acheter un super disque SSD. Au moment de passer en caisse, il sort sa carte bancaire, le caissier l'insère dans son terminal de paiement et le client doit, après avoir regardé au passage la somme qu'il s'apprête à débourser, saisir son code confidentiel (le code ***PIN***). Ce code est directement vérifié par la carte (plus exactement par la puce contenue dans la carte). Le client dispose de trois tentatives consécutives pour entrer le bon code. Après trois échecs, la carte se bloque.

Si le code est bon, les opérations suivantes ont lieu :
1. Le terminal se connecte au serveur de la banque X et envoie une ***demande d'autorisation*** de paiement contenant le numéro de la carte bancaire ainsi que le montant de la transaction.
2. Le serveur de la banque X regarde le numéro de la carte et, s'il ne s'agit pas d'une des cartes qu'il a émises, envoie le numéro de carte avec le montant de la transaction au serveur de la banque Y, via le réseau interbancaire permettant de relier les différentes banques. C'est le réseau interbancaire qui route la demande d'autorisation grâce au numéro de carte dont les premiers chiffres correspondent à l'émetteur de la carte. Si c'est une carte que sa banque a émise, alors le serveur de X traite la demande en interne.
3. Le serveur de la banque Y prend connaissance du numéro de la carte bancaire et vérifie que le compte correspondant à ce numéro dispose d'un solde suffisant pour honorer la transaction. D'autres *vérifications* peuvent être réalisées.
4. Si c'est le cas, il répond à la banque X que le paiement est autorisé. Si ce n'est pas le cas, il répond le contraire.
5. Enfin, le serveur de la banque X transmet la réponse au terminal du commerçant.
6. La transaction est validée ("paiement autorisé") ou refusé ("paiement non autorisé").

1.2 La demande d'autorisation

La suite des opérations décrites ci-dessus se nomme la "demande d'autorisation" et a essentiellement pour but de vérifier que le compte client est bien provisionné, etc. Cette suite d'opérations montre que le rôle des banques est double.
En effet, l'action de la banque diffère selon si la demande d'autorisation est locale ou non.
i) Si ce n'est pas le cas, son rôle est d'acheminer la demande vers la banque qui a la capacité de la traiter.
ii) Si la demande d'autorisation est locale, son rôle est de vérifier que celle-ci peut être honorée et de produire une réponse qui est ensuite acheminé vers le terminal du commerçant depuis lequel la demande a été émise.

Chaque banque est donc composée de *deux serveurs*.
Le ***serveur d'acquisition*** : il s'agit du serveur de la banque du commerçant auquel se connecte le terminal via le réseau téléphonique. Une fois connecté, le terminal envoie au serveur d'acquisition toutes les informations concernant la transaction, notamment le montant, le numéro de carte et des données permettant d'assurer la sécurité de la transaction. Le serveur d'acquisition a ensuite pour rôle d'acheminer les données vers un autre serveur capable de les traiter.
Le ***serveur d'autorisation*** : il s'agit du serveur de la banque du client auquel le serveur d'acquisition transmet la demande d'autorisation de paiement émise par le terminal. C'est lui qui est chargé de produire la réponse à la demande d'autorisation. Cette réponse suit donc le chemin inverse, c'est à dire : serveur d'autorisation de la banque du client -> serveur d'acquisition de la banque du commerçant -> terminal du commerçant.

1.3 Le routage

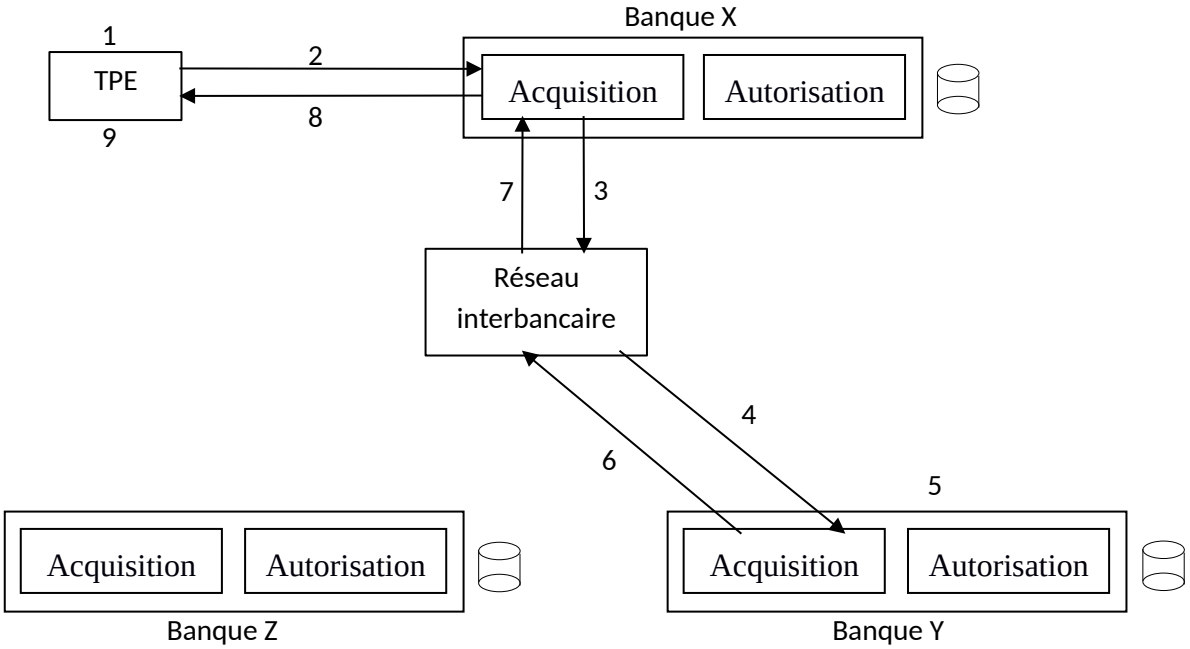
Pour effectuer le routage des demandes d'autorisation, c'est-à-dire pour déterminer à quelle banque chaque demande d'autorisation doit être transmise, le serveur d'acquisition utilise les premiers numéros de chaque carte bancaire concernée : ceux-ci indiquent la banque ayant émis cette carte.
Dans ce projet, nous aurons les principes suivants :
– un numéro de carte est constitué de seize chiffres décimaux ;
– les premiers correspondent à un code spécifique à chaque banque (voir **Annexe**) ;
– les serveurs d'acquisition des banques sont directement reliés au réseau interbancaire.

Chaque serveur d'acquisition analyse donc le numéro de la carte qui figure dans la demande d'autorisation qu'il reçoit, puis :
– si le client est dans la même banque que le commerçant (et que le serveur d'acquisition), il envoie la demande directement au serveur d'autorisation de cette banque ;
– si le client est dans une autre banque, le serveur d'acquisition envoie la demande sur le réseau interbancaire, sans se préoccuper de la suite du transit.

Le réseau interbancaire n'est donc pas un simple réseau physique. On peut parler de système interbancaire. Il doit aussi effectuer le routage des demandes d'autorisation, c'est-à-dire analyser les demandes qui lui sont fournies, envoyer chaque demande vers le serveur d'acquisition de la banque correspondante et, enfin, prendre en charge la transmission de la réponse lorsqu'elle lui revient.

2 Résumé

Le schéma suivant donne une illustration des étapes réalisées lors d'une demande d'autorisation.



Étapes :
1) Le TPE récupère les informations sur la carte bancaire et le porteur puis effectue un ensemble de vérifications (numéro de carte valide, ...).
2) Le TPE envoie la demande d'autorisation au serveur d'acquisition de sa banque (la banque X).
3) Supposons que le porteur est dans la banque Y. Le serveur d'acquisition qui n'a pas accès directement la banque Y (qui a ici le rôle d'émetteur) à va alors envoyer la demande au serveur du réseau interbancaire.
4) Le réseau interbancaire qui a connaissance des serveurs d'acquisition de toutes les banques, route la demande au serveur d'autorisation de la banque Y.
5) Le serveur d'acquisition de la banque Y reçoit la demande et l'envoi à son serveur d'autorisation qui effectue un ensemble de vérifications concernant la carte (elle ne doit pas être mise en opposition) et le compte bancaire du porteur. Supposons que ces tests sont concluants, le serveur génère alors un numéro d'autorisation. Il stocke ensuite des informations sur cette autorisation dans sa base de données.
6) Le numéro d'autorisation est retourné (si la demande d'autorisation a échouée, un code d'erreur est retourné).
7) Le numéro d'autorisation est retourné au serveur d'acquisition de la banque X.
8) Le numéro d'autorisation arrive jusqu'au TPE.
9) Le TPE stocke les informations de la transaction.

Le terminal peut être classique (TPE) ou virtuel (TPEV) afin de simuler un paiement sur le Web.
Les premiers chiffes du numéro de carte bancaire indiquent la banque émettrice c'est-à-dire qui détient le compte associé à la carte (voir **Annexe**).

Annexe - Numéro de carte bancaire

Un numéro de carte bancaire est composé de 16 chiffres :

ABCD EFGH IJKL MNOP

A indique le réseau émetteur de la carte
Exemples : 3 pour American Express, 4 pour Visa, 5 pour Mastercard

BCD identifient à la banque émettrice (le BIN)
Exemples : 131 pour Crédit Agricole, 132 pour Crédit Mutuel, 970 pour La Banque Postale, 972 pour LCL, 973 pour Société Générale, 974 pour BNP, 978 pour Caisse d'Épargne, 975 pour La BRED.
Remarquons que la longueur de cet identifiant est variable, il peut aller jusqu'à 5 chiffres mais nous nous limiterons à 3 comme les exemples.

Ensuite, les chiffres correspondent au numéro de compte individuel.

Le dernier chiffre est la clé de Luhn. C'est un checksum pour vérifier qu'il n'y a pas d'erreur de saisie du numéro de carte.

Annexe - Base(s) de données

il faudra une (ou plusieurs) bases de données pour stocker les informations nécessaires au fonctionnement du simulateur.

La (les) base(s) de données permettra (permettront) de stocker notamment :

- les informations sur les cartes bancaires (numéro de carte, date d'expiration, id du compte associé, bloquée ou non, le code PIN et/ou le cryptogramme visuel, ...)

- les transactions de chaque TPE (numéro d'autorisation, montant, id banque/BIN, ...)

- les comptes bancaires de chaque banque (pour chaque compte : numéro de compte, nom, prénom, solde, éventuellement montant plafond, en cours, ...).

- les autorisations délivrées par une banque (pour chaque autorisation : numéro d'autorisation, id compte, date, montant, id du commerçant, ...)

- les cartes en opposition.

C'est à concevoir.

Annexe – Quelques liens vers des documents intéressants

https://www.comprendrelespaiements.com/abc-de-la-monetique-les-acteurs-et-leurs-roles/
https://www.comprendrelespaiements.com/les-systemes-de-paiement-le-modele-a-4-coins/
https://www.comprendrelespaiements.com/modele-a-4-coins-echanges-de-flux-pour-un-paiement-par-carte/