



**M-PORTEFEUILLE :
LE PORTEFEUILLE ÉLECTRONIQUE MOBILE LIPSO**

UNIVERSITÉ DE MONTRÉAL

**PRÉSENTÉ PAR
CHRISTINA BRAZ ET EQUIPE LIPSO**

LE 17 JUIN 2003



M-PORTEFEUILLE : LE PORTEFEUILLE ÉLECTRONIQUE MOBILE LIPSO

La téléphonie mobile est l'une des plus importantes innovations technologiques depuis l'avènement de la télévision et de l'ordinateur personnel. Plusieurs experts en télécoms croient que la messagerie mobile deviendra un outil de communication puissant qui améliorera la productivité des entreprises.

La messagerie texte mobile consiste en de courts messages d'un maximum de 160 caractères. Il s'agit aussi d'un mode rapide, discret et pratique de communication lorsque l'on ne peut pas ou ne veut pas placer un appel vocal. Durant le seul mois de novembre 2002, les canadiens ont envoyé 20 millions de messages courts, une augmentation de 98 % depuis l'introduction de la messagerie texte mobile inter réseaux au Canada en avril par les quatre plus importants télécommunications sans fil canadiens. L'expansion est partout dans le monde, et surtout au Japon, Asie du sud-est et en Europe (voir Tableau 1).

I- MANDAT

Notre mandat consiste à proposer à la compagnie LIPSO, une solution permettant d'effectuer des transactions à partir d'un téléphone portable (M-Portefeuille), en utilisant la technologie de LIPSO pour le transfert et le traitement des SMS.

Pour réaliser ce mandat, notre méthode consistera dans un premier lieu à définir les différentes étapes d'une transaction, analyser ce qui existe sur le marché et identifier les contraintes liées à chaque étape du processus. À partir de cette étude, différents scénarios seront proposés, ces derniers seront par la suite analysés et validés par LIPSO, afin de définir un processus de transaction par SMS, détaillé et validé selon les contraintes actuelles.

La seconde étape consistera à analyser ce processus afin de définir :

- L'ergonomie du système;
- Les éléments de sécurité à implanter;
- La méthode de facturation à utiliser;
- Les éléments du modèle d'affaires qui en découle.



Enfin la troisième étape consiste à réaliser, en collaboration avec les architectes de LIPSO, un prototype qui permettra de visualiser le processus de manière plus concrète. Nous avons commencé par analyser le fonctionnement des SMS, les processus utilisés par LIPSO et l'état de la situation dans le monde en ce qui concerne le M-Commerce. Cela nous a permis d'arriver à la conclusion qu'il n'existe actuellement pas de véritables moyens de transiger à l'aide des SMS. Les solutions actuelles de M-Commerce permettent en fait d'utiliser les SMS pour simplifier ou ajouter de la valeur à des transactions effectuées sur Internet. Cependant à partir des diverses utilisations des SMS existantes notamment en Europe, il est possible d'identifier des solutions pour diverses étapes du processus de transaction. Les étapes suivantes de l'analyse seront fonction d'un découpage du processus de transaction que nous sommes en train de réaliser tout en respectant les contraintes et leurs implications.

II- LIPSO¹

II-1. Historique

LIPSO Media, dont le siège social est situé à Montréal, a été fondée en mars 2000 par Vivianne GRAVEL et Louis BRUN. Le 11 décembre 2002 - LIPSO et Investissement Desjardins ont annoncé la réalisation d'un financement de 1,5 M\$ afin d'appuyer les efforts de commercialisation de LIPSO et le développement de sa technologie innovatrice de messagerie texte mobile.

II-2. Mission et Organisation

LIPSO se veut le leader mondial dans le développement des solutions de connectivité SMS, EMS et MMS permettant aux entreprises d'échanger des données critiques avec leurs usagers mobiles (employés, fournisseurs et clients). L'entreprise est formée d'un conseil d'administration, une équipe de gestion et une équipe des opérations (architectes et programmeurs).

¹ Toutes les informations de cette section sont reprises du site de LIPSO : <http://www.lipso.com>

II-3. Produits, Services et Expertise

i-LIPSO : LIPSO a développé un routeur SMS/MMS innovateur, robuste et performant, ce routeur traite 5 000 messages textes des cellulaires à la seconde et facilite la transmission de données entre les réseaux IP et les réseaux mobiles. La grande flexibilité des protocoles d'entrée et de sortie du logiciel de routage multi-applications et multi réseaux de LIPSO constitue son grand avantage concurrentiel puisque ce logiciel qui est indépendant de la technologie des opérateurs télécoms et des constructeurs de cellulaires, permet d'acheminer des messages sur tous les principaux réseaux sans fil existants, quels que soient les infrastructures et protocoles de communications utilisés (CDMA, TDMA, GSM).

Les champs d'application de la solution i-LIPSO :

Solutions d'affaires pour les entreprises de distribution

- Alertes SMS reliées à ERP;
- Système d'inventaires - notification aux forces mobiles;
- Logistiques.
- Solutions de Gestion
 - Courriels corporatifs;
 - Notifications étapes de projet - gestion de projet;
 - Alertes priorités hebdomadaires;
 - Alertes session de formation et meeting.
- Solutions d'affaires pour le secteur bancaire
 - Carte de crédit : alertes cartes perdues et retrouvées;
 - Notification SMS sur délais limite de paiement de comptes;
 - Information sur compte ou balance et transactions bancaires.



- Solutions d'affaires en relations clients
 - CRM - alertes personnalisées;
 - E-catalogue - statut de livraison;
 - Promotions;
 - Invitations spéciales et club privilégié;
 - Information sur les retards (vols, etc.)
- Solutions pour le secteur de divertissement
 - Courriel : accès et messagerie instantanée;
 - Grands titres de l'information : trafic;
 - Cotes en bourse;
 - Température;
 - Divertissements : cinéma, sport, réservation de billets (avions, train, hôtels);
 - Radio : Concours via SMS;
 - ITV : votes par SMS.

Expertise : LIPSO met à la disposition des clients une équipe qui offre

- Analyse des besoins des clients en terme de communication mobile;
- Agence ou développe des solutions de connectivité qui correspondent à l'architecture actuelle du client;
- Maximise la performance des communications mobiles.

II-4. Clients et Partenaires

LIPSO a trois (3) catégories de partenaires :

- Manufacturiers d'infrastructures en télécommunication;
- Manufacturiers d'infrastructures IP et TI;
- Intégrateurs (e-business) et firmes de consultation TI.

Les plus importants comptes clients de LIPSO sont :

Invertix Corp : LIPSO a contribué avec sa solution au développement d'une application Internet qui permet l'envoi instantané des messages aux PC et aux périphériques sans fil.

IQ investissement Québec: LIPSO a délivré la solution m-promotion, qui permet aux membres de recevoir sur leurs mobiles, pagers, etc. des alertes publicitaires.

TVA (émission Star Académie) : Rogers AT&T communication sans fil en partenariat avec LIPSO ont conçu le système de votes par messagerie SMS sans fil.

III- PROBLÉMATIQUE D'AFFAIRES

III-1. Contexte

LIPSO qui est déjà un pionnier et un leader des solutions de connectivité mobile au Québec, veut franchir un autre pas vers la découverte d'autres créneaux pour la création de la valeur. Et c'est dans ce contexte là, que LIPSO a délégué le mandat décrit précédemment. Le souci majeur est de garder sa position d'innovateur. Ainsi, LIPSO se voit aujourd'hui poussée à investir dans la recherche et développement d'une solution qui lui permettra d'aller encore plus loin dans la technologie sans fil en élaborant un système de paiement par mobile. La prochaine étape de LIPSO est de réaliser un M-Portefeuille qui permettra de faire des transactions SMS par le biais du mobile.

III-2. Enjeu

LIPSO possède une solide connaissance des différentes solutions m-business proposées sur le marché, elle offre des solutions de connectivité permettant aux entreprises d'étendre ses communications clés vers leurs employés, leurs fournisseurs et leurs clients en mouvement en reliant les réseaux IP et mobiles.

L'introduction d'un M-Portefeuille dans l'offre de service de LIPSO ne pourra que contribuer à augmenter les ventes, créer de la valeur pour les entreprises et opérateurs mobiles en plus d'offrir à l'utilisateur final un système simple, rapide, efficace, sécuritaire à faible coût et surtout mobile.

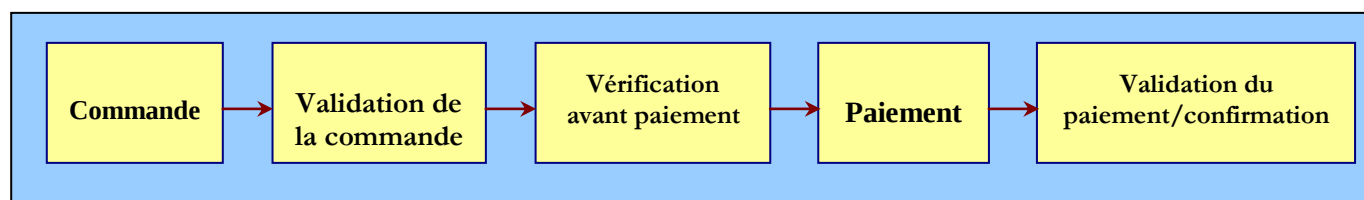
IV- STRATÉGIE

IV-1. Description

La stratégie adoptée par notre équipe pour répondre au mandat délégué par LIPSO consiste à modéliser le processus de transactions en blocs. Ce processus de transactions sera générique et pourra répondre par la suite à toutes les applications qui peuvent être mises en place. La validation de ce processus sera établie conjointement avec les membres de LIPSO (Francis et Louis) par le biais de divers scénarios.

Le processus de transactions comporte cinq éléments :

- Commande;
- Validation de la commande;
- Vérification avant paiement;
- Paiement;
- Validation du paiement et confirmation.



En fait, quatre scénarios sont présentés pour le processus de transactions. Tout scénario sera décrit pour relever les avantages et les inconvénients de chacun. Cette stratégie a permis de retenir deux scénarios en collaboration avec LIPSO (scénario bancaire et scénario prépayé). Vers la fin, un seul scénario doit être retenu et sur lequel un prototype va être bâti.

IV-2. Approche et Méthodologie

IV-2.1 Sécurité

À ce niveau, il importe d'identifier une solution de sécurité qui exploite ce qui existe dans le marché en parcourant les contraintes et leurs implications. Pour cet axe, la portion localisée entre LIPSO et l'Internet sera abordée. Ainsi, cette partie sera traitée sur tous les niveaux, puisque c'est elle qui affecte particulièrement LIPSO et non toute la chaîne des intervenants. En fait, la délimitation de cette zone d'action a été une des nos préoccupations majeures afin de bien définir le cadre d'axe de sécurité.

À l'heure actuelle, il existe plusieurs menaces de sécurité dans le domaine du SMS tels que le SMS Spam, le SMS Spoofing, le SMS Virus, la problématique des clés statiques et courtes. L'authentification est un des points les plus sensibles à l'égard de l'utilisateur du système. Les caractéristiques sophistiquées des produits SMS les plus performants ouvrent la porte pour des nouveaux trous de sécurité.

IV-2.2 Procédé de transaction

À travers les différentes réunions avec LIPSO, il importe de développer un procédé de transactions générique (ce qui élimine de penser à une application spécifique et bâtir la solution) puisque ils pourront l'adapter à une multitude d'applications. Il faut donc analyser les différents processus de transactions ainsi que les contraintes qui y sont attachées.

IV-2.3 Ergonomie du service

Pour cet axe, il faut prévoir une adéquate ergonomie du service afin de proposer à l'utilisateur une bonne convivialité de l'application (GUI) et réduire au minimum la quantité d'écrans nécessaires à la finalisation de la transaction car la taille des périphériques mobiles (téléphones cellulaires, PDAs, etc.) est réduite et les claviers sont difficiles à manipuler.

Le but est de développer un prototype de la solution où deux membres de l'équipe de développement de LIPSO seront responsables (Bruno et Pascal). Pour cette activité, nous essayerons d'obtenir l'aval d'un opérateur mobile pour fournir des appareils pour le prototype et les tests.

En conclusion, l'élaboration d'une solution de service SMS transactionnel, même si elle est générique, suivie de la réalisation d'un prototype est une bonne approche. Toutefois, cette solution doit répondre aux attentes de LIPSO. En effet, une solution générique de portefeuille mobile (M-Portefeuille), a pour but de répondre aux besoins de LIPSO, et reste une solution extensible où on peut greffer plusieurs applications spécifiques. LIPSO pourra devenir un fournisseur de services cellulaires (MSP) à long terme en offrant une solution complète à ses clients.

V- CONTRAINTES, IMPLICATIONS ET CONSTATATIONS

V-1 Contraintes et Implications

Le marché du m-commerce (ou mobile commerce) ne décolle toujours pas. Et cela bien que tous les opérateurs européens proposent une solution de micro paiement par téléphone portable. La raison est simple : un marchand comme Amazon.com doit aujourd'hui se relier à pas moins de vingt-cinq plates-formes techniques différentes pour couvrir l'Europe.

L'interopérabilité de messages SMS : Depuis novembre 2001 les quatre fournisseurs canadiens de téléphonie mobile ; Bell Mobility (30% CDMA), Microcell Connexions (10% GSM), Rogers AT&T Wireless (30% TDMA ou GSM) et Telus Mobility (30% CDMA) sont arrivés à un accord pour que leurs abonnés puissent échanger des messages SMS, d'un réseau à l'autre. Ainsi les opérateurs canadiens ont joint l'initiative des opérateurs américains ce qui a permis de déclencher l'explosion du marché SMS en Amérique du nord. On peut s'attendre et voir le fort échange entre marché canadien et américain à une interopérabilité des messages textuelles entre les deux pays.

Convivialité de la solution : Beaucoup de solutions n'ont pas été retenues pour manque de simplicité. En effet, échanger 4 ou 5 messages pour accomplir une transaction entrave vraiment son développement.

Coût de la solution : il faut que le nombre de messages échangés par l'utilisateur et facturés soit proportionnel au montant de la transaction.

Nombre d'intervenants : En l'absence de standard de paiement fourni par les opérateurs, la solution doit limiter le nombre d'intervenants entre institution financière, opérateur, le fournisseur d'application, hébergeur, etc.

Standardisation de la solution : Le m-commerce a du mal à se développer à cause du manque d'interopérabilité de messages SMS. En fait, presque tous les opérateurs mobiles dans le monde offrent des solutions de micro paiement. Sauf qu'elles sont toutes différentes. Il faut donc créer un protocole standard pour gérer ces transactions. Il existe aussi des solutions basées sur des modifications hardware ou sur l'usage de cellulaires propriétaires comme celle de Benefon. Ces solutions ne peuvent réussir. Parmi ces solutions, on peut citer celle offerte par MasterCard basée sur l'insertion d'information de la carte de crédit dans la carte SIM ou l'ajout au portable d'un lecteur de carte.

V-2 Constatations

Les méthodes de paiement les plus répandues dans le cas du m-commerce utilisant SMS est le off line (facture de téléphone) dans le cas du post-paiement (le cas du Japon) et la déduction de la carte prépayé (Europe).

La méthode de paiement qui inclut la transmission sécurisée de numéro de la carte crédit par SMS n'est pas prévue pour les années prochaines. En fait, il a fallu du temps afin que les gens s'habituent à envoyer les renseignements personnelles à travers Internet. Il faudra aussi prendre en considération que la plupart des gens préfèrent encore la transmission des numéros de la carte de crédit par téléphone suite à une publicité par SMS.

Une application m-commerce qui a des fortes chances de décoller est le remplissage des cartes prépayées par SMS. Cette opération a été testée avec succès en République Tchèque. A travers l'utilisation des SMS les opérateurs ont pu réduire les coûts et partageront cette réduction avec le client afin de bénéficier d'un avantage compétitif.

Afin de pousser ce type de commerce, on pourra donner aux utilisateurs de service SMS des rabais afin de les habituer à l'usage de ce nouveau service. Cette méthode est applicable si le marché cible est sensible au prix.

La multitude des technologies mobiles implique la fédération d'un outil ou d'une entité afin de gérer et permettre l'interopérabilité. Finalement, les biens à commercialiser par SMS ne doivent pas dépasser un certain montant (100\$) pour la simple raison que le service est nouveau et ça nécessite une certaine maturité dans le marché.

En voici quelques solutions implantées à travers le monde :

- i-mode (NTT DoCoMo) Japon;
- EZWeb (KDDI) Japon;
- J-sky (J-Phone) Japon.

Le tableau qui suit présente le volume des messages SMS échangés au niveau mondial en 2000 ainsi que le nombre de SMS par usager et par mois.

	Messages Texte (millions)	SMS/Utilisateur/Mois
Europe Ouest	40.7	17
Japon	30.0	47
Phillippines	10.5	194
USA	1.5	1.3
China	0.8	0.4
ROW	14.1	6
Monde Entier	97.6	14

Tableau 1 : Statistiques 2000 sur les SMS à travers le monde².

VI- SCÉNARIOS

En s'appuyant sur la stratégie retenue précédemment et en gardant dans l'esprit la nécessité de développer une solution générique ; souple, flexible et la plus proche des réalités du marché, on a élaboré plusieurs scénarios inspirés des solutions existantes et adaptées à la spécificité des contraintes actuelles. Ainsi, quatre scénarios ont été mis en place. Les deux derniers scénarios ont capté l'attention de LIPSO et ce sont eux qui seront développés en citant les avantages et les inconvénients de chacun.

² Mobile data and m-commerce in Europe (a mobile network operators revenue perspective, 1999-2003)
<http://www.crt.dk/uk/staff/chm/wap/sms.pdf>

VI-1 Scénario 1

Processus de transaction : Il faut distinguer entre le micro et le macro paiement. Pour le micro paiement, les solutions généralement utilisées sont basées sur l'usage d'un compte pré-établi et enregistré chez le fournisseur de l'application (LIPSO dans notre cas). Une autre solution consiste à ajouter le prix de la transaction à la facture téléphonique de l'abonné. Pour les macro paiement, disposer d'un compte d'argent chez LIPSO n'est pas la meilleure solution. Les deux solutions qui peuvent être envisagées sont : le client ouvre un compte chez LIPSO et communique les informations concernant sa carte de crédit, ainsi lors des transactions l'utilisateur n'a pas à transmettre sur le réseau ses informations confidentielles. La deuxième alternative est de contacter l'institution financière du client, elle se charge d'envoyer une demande de confirmation du client, qui en faisant un accusé il sera transféré à LIPSO et qui à son tour envoie le message de confirmation du succès de la transaction à l'utilisateur.

Bloc du processus :

- Micro paiement (1\$ à 30\$) : négociation, le client envoie un message de confirmation avec son code PIN, la somme sera déduite du compte et un message de succès de la transaction est envoyé.
- Macro paiement (31\$ et plus) : négociation, le client envoie un message de confirmation avec son code PIN, LIPSO envoie un ordre de paiement à l'institution financière, cette dernière envoie un message de demande de confirmation au client, un accusé de confirmation, l'institution financière confirme à LIPSO le succès de la transaction, message de retour au client pour confirmation. La particularité de ce scénario est la nécessité de la tenue d'une base de données des utilisateurs chez LIPSO. Ces utilisateurs devront adhérer à LIPSO en fournissant des informations personnelles afin de bénéficier du service transactionnel par SMS.

VI-2 Scénario 2

Ce scénario diffère du scénario précédent dans la mesure où la base de données ne réside pas chez LIPSO. Cette tâche est départagée entre les institutions financières et les marchands. Un utilisateur doit contacter un marchand ou une institution financière pour s'inscrire. Sans inscription, il ne peut bénéficier du service m-LIPSO. Le client peut payer de différentes manières :

- Numéro de carte de crédit : problème de sécurité.
- Banque via mot de passe, voir exemple de FIDO et Banque Royale : problème d'obtenir un accord avec les différentes banques.
- Fournisseur de service cellulaire : Serait-il raisonnable de demander à des Rogers ou Bell de gérer des milliers de paiements.

Il semble plus intéressant à cette étape d'utiliser un tiers de paiement spécialisé dans le domaine, avec peut être un système de cartes prépayés. En fait, nous distinguons essentiellement deux scénarios de paiement. Un des scénarios offre au client la possibilité d'avoir un portefeuille virtuel prépayé et l'autre assure un lien d'une part entre le marchand et le client et d'autre part entre le marchand et l'institution financière du client.

Dans cette partie, nous allons plus particulièrement présenter un scénario dans lequel interviennent le client, le marchand et leurs institutions financières. De façon générale, nous avons les intervenants suivants :

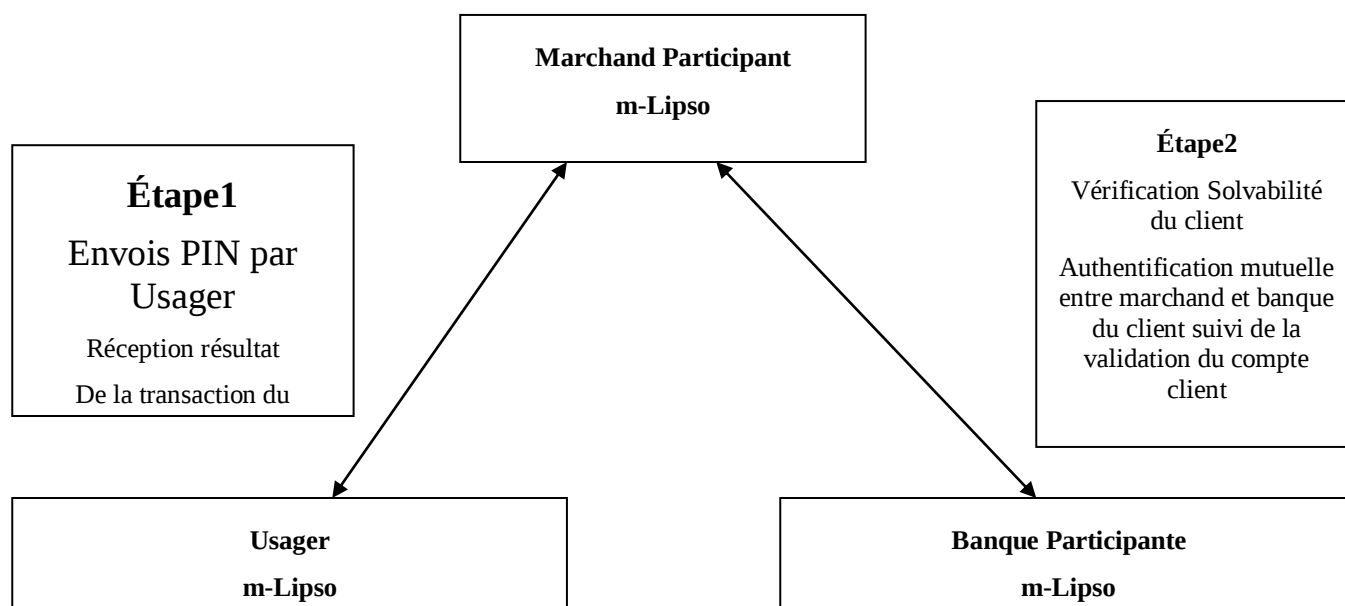
- L'utilisateur ou le client;
- Les banques participantes;
- Les marchands participants;
- LIPSO et sa technologie.

Le client d'une banque participante peut relier son compte m-Lipso à son/ses compte(s) courant(s). Le compte m-Lipso peut avoir un numéro d'identification semblable à celui du téléphone du client. Ceci assure l'unicité du compte.

Étape 0 : Le client passe sa commande auprès d'un marchand participant. Si sa commande, ne dépasse pas un certain montant présélectionnée, elle est sauvegardée au niveau du m-Lipso, la validation est faite de façon authentique à travers son numéro de téléphone.

Étape1 : Si l'achat est supérieur à la limite de non validation, Le client doit rentrer un code d'authentification pour continuer la transaction. Le client soumet un code PIN dans le système de paiement du marchand affilié par SMS. Pour cette étape, le message SMS peut être facturé au marchand.

Étape2 : La vérification du PIN est faite au niveau du marchand par le m-Lipso qui y est installé. Cette vérification se fait par communication IP avec la Banque du client. Le réseau utilisé peut être un VPN sécurisé. Cette vérification doit aussi prendre en compte l'identité réelle du marchand. Une fois les vérifications terminées, un SMS est envoyé au client pour lui annoncer que la transaction est soit acceptée ou refusée. Dans le cas d'une transaction acceptée, un message de confirmation couplé à un code de transaction lui sont envoyés. m-Lipso retient un pourcentage sur toute transaction complétée (Voir Schéma3 qui suit).



Ce scénario permet à LIPSO de pouvoir assurer la sécurité des informations puisqu' aucune information cruciale n'est transmise là ou elle n'a pas de contrôle, c'est à dire entre le client et son fournisseur de sans fil. De plus cela peut permettre à des clients de banques diverses ou de fournisseurs divers de transiger.

³ Ce schéma de scénario s'inspire de celui de l'entreprise paybox : www.paybox.ne, www.mint.nu, www.mobipay.com .

VI-3 Scénario Bancaire

M-LIPSO est un service de SMS qui permet aux utilisateurs mobiles d'effectuer le paiement en ligne, en toute sécurité et confidentialité. Il offre un niveau additionnel de sécurité pour le paiement en ligne, permettant l'authentification de toutes les parties de la transaction. Le scénario de transactions contient cinq intervenants majeurs :

- Le client utilisant SMS sur son mobile.
- Les opérateurs télécoms.
- LIPSO.
- Les marchands.
- Les institutions financières que ça soit les banques, les émetteurs de cartes de crédit ou autres.

Il faut signaler à ce stade que les opérateurs télécoms, les marchands et les institutions financières adhèrent à la solution que LIPSO propose. A cet effet, un code sera attribué pour chaque organisme (1415 pour marchand1, 1416 pour marchand2, 2014 pour institution financière 1, 2015 pour institution financière 2...)

L'approche de M-LIPSO en matière de facturation décharge les opérateurs mobiles et fournisseurs de contenu de toute responsabilité. Les modèles traditionnels obligent les opérateurs/fournisseurs à traiter tous les transferts de fonds et à accepter la responsabilité d'une transaction lorsqu'un(e) acheteur(e) ne peut acquitter son paiement. De ce fait, à l'occasion de chaque transaction, l'opérateur mobile ou fournisseur de contenu se trouve à pratiquement donner un prêt sans aucune garantie. M-LIPSO les libère de cette responsabilité. Il authentifie et autorise en temps réel chaque utilisateur, puis demande l'approbation de la transaction par l'institution financière appropriée. M-LIPSO utilise des modes de paiement connus des clients et dignes de confiance, et en assure un niveau de sécurité adéquat pour combattre toute tentative de fraude.

M-LIPSO recueille le paiement des utilisateurs mobiles, ainsi les utilisateurs M-LIPSO peuvent recevoir une facture unique pour toutes les transactions réalisées par l'entremise de leurs appareils mobiles, et les fournisseurs de contenu n'ont pas besoin de les facturer directement. Cet arrangement proportionnera aux fournisseurs de contenu une réduction des dépenses et des risques en encourageant à constamment présenter des nouvelles offres aux utilisateurs mobiles, et par conséquent en améliorant leurs profits. En outre, M-

LIPSO générera des revenus supplémentaires en prélevant 8% de commission afin d'administrer le processus de facturation.

Avantages

Paiement : Décharger les intervenants du processus de paiement et laisser les institutions financières s'en occuper. Ceci encouragera les clients ainsi que les marchands pour adhérer et utiliser la solution facilement. M-LIPSO décharge les opérateurs mobiles, fournisseurs de contenu de toute responsabilité : transferts de fonds et à accepter la responsabilité d'une transaction lorsqu'un(e) acheteur(e) ne peut acquitter son paiement. C'est une solution globale et non pas locale : L'accès et le paiement est disponible en tout temps et en tout lieu. Fonctionnant par le biais des SMS, le service M-LIPSO peut être utilisé pour effectuer des transactions via le Web et via l'appareil mobile n'importe où dans le monde.

Sécurité : Le processus de transaction est sécurisé du fait qu'aucune information critique ne transige au niveau du réseau. En plus, la solution de LIPSO aura des points d'accès bien définis avec les différents intervenants ce qui facilitera la détection des imperfections (points d'intégrations avec les institutions financières, les opérateurs télécoms et les marchands). M-LIPSO authentifie et autorise en temps réel chaque utilisateur, puis demande l'approbation de la transaction par l'institution financière appropriée.

Nombre d'intervenants : Chaque intervenant se concentrera sur sa spécialité et offrira la meilleure intégration pour la solution retenue.

Transaction : LIPSO se positionne entre le réseau Mobile et le réseau IP. Ceci démarque LIPSO en tant que fournisseur de solutions entre les deux réseaux. Le premier réseau a pour but de véhiculer les messages SMS et le deuxième a pour mission de procéder au paiement.

Légal : Les informations personnelles sensibles des clients ne sont stockées qu'au niveau de l'institution financière. Ceci permet au client d'effectuer ces transactions sans crainte de dévoilement de leurs renseignements personnels.

Logistique : Aucun frais de logistique n'est associé au scénario bancaire (pas d'impression, pas de distribution, pas de gestion de compte, pas de gestion du personnel hors domaine de qualification).

Solution : En ayant une solution avec un noyau dur et des passerelles vers les différents intervenants, la flexibilité et l'évolutivité de la solution est garantie grâce à la modularité de la solution.

Application : Le portefeuille virtuel ou M-LIPSO, est hébergé dans le serveur central dont l'avantage est un faible coût de maintenance et un audit total des transactions.

Modèle d'affaire : Grâce à M-LIPSO, les opérateurs sans fil ont accès à une multitude d'occasions d'affaires. M-LIPSO intègre les réseaux sans fil à ceux des institutions financières, forgeant ainsi un réseau intégré qui permettra aux opérateurs mobiles, fournisseurs de contenu, LIPSO et même les institutions financières d'exploiter les nouveaux marchés qu'offre le commerce mobile. En offrant un système de paiement au client basé sur l'institution financière, les opérateurs de réseau peuvent mettre à la disposition des banques et des marchands de nouveaux circuits de vente.

Inconvénients

Nombre d'intervenants : Le nombre d'intervenants est un facteur de sensibilité quant au partage de la responsabilité et aussi en termes de création et de partage de la valeur.

Légal : Ce scénario ne garantit pas l'anonymat du client puisqu'il est connu par les différents intervenants.

Intervenants

Client : Avoir d'autres possibilités pour effectuer ses achats (gagner du temps, la mobilité).

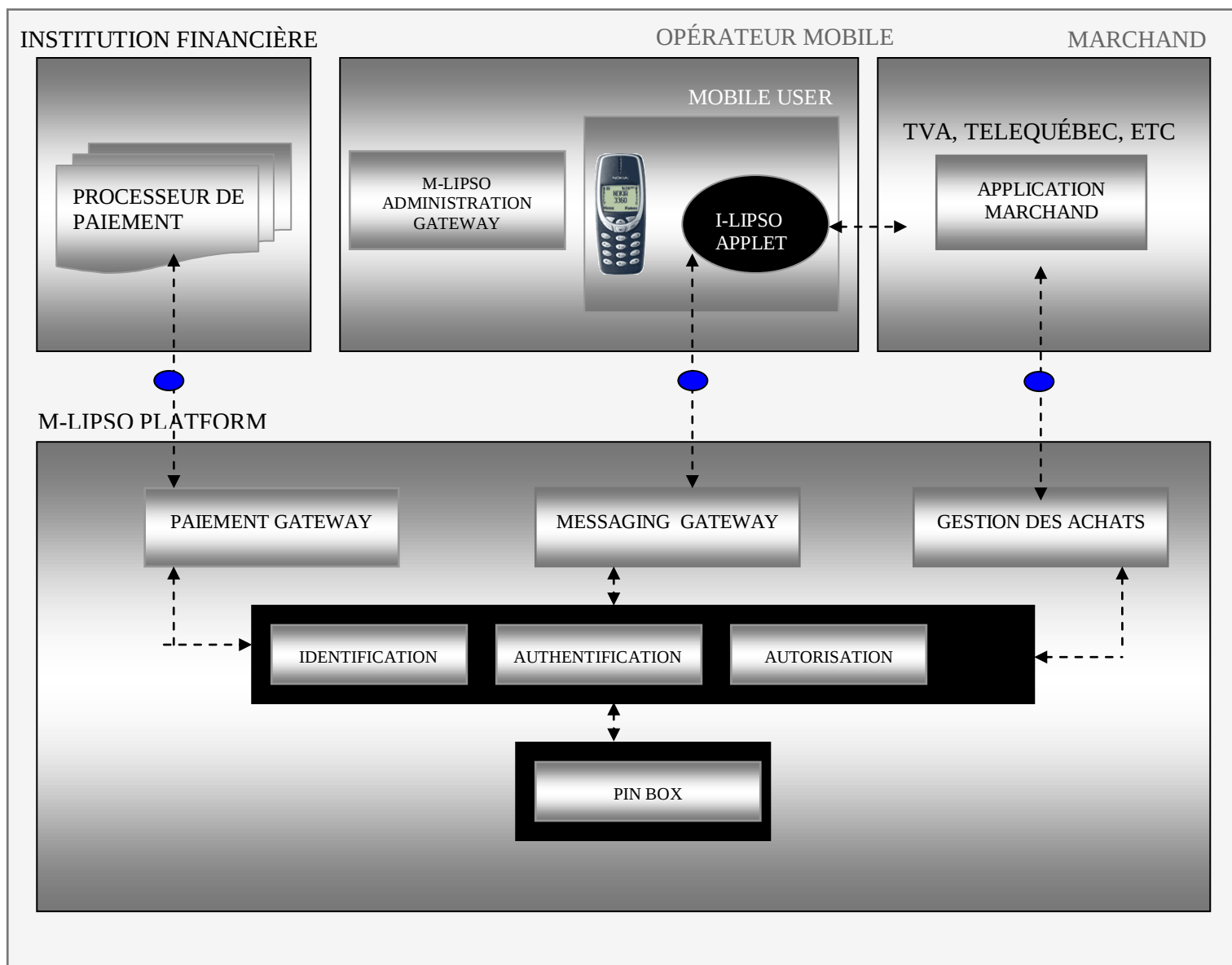
Opérateur Télécoms : Un gain supplémentaire en terme de messages SMS véhiculés grâce au SMS transactionnel.

LIPSO : Prélèvement d'un pourcentage sur chaque transaction effectuée par le client.

Marchand : Développer un autre créneau de distribution et par la suite générer plus de profits et atteindre plus de gens.

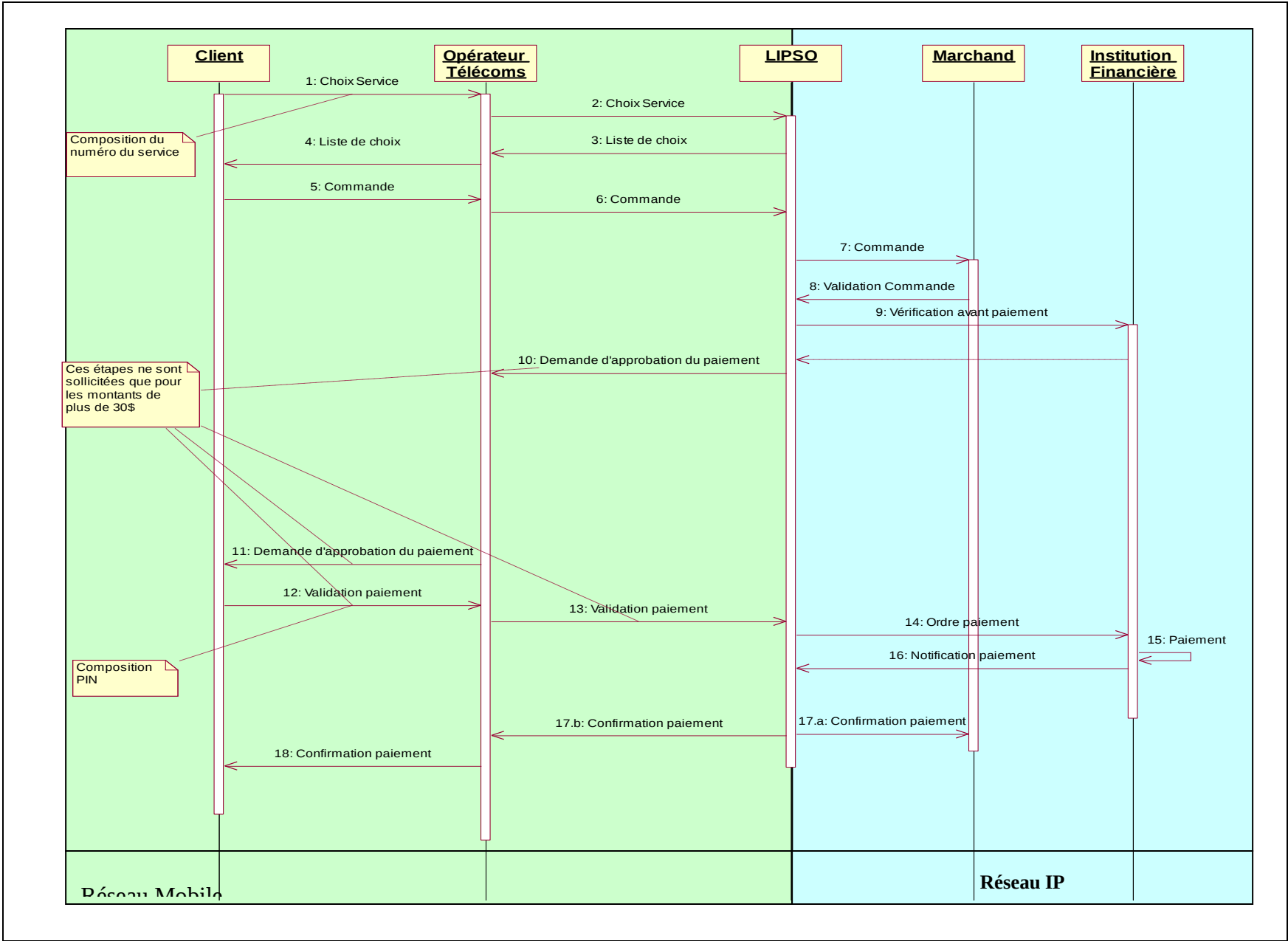
Institution financière : Proposer ce service à ses clients et attirer d'autres clients intéressés par le SMS transactionnel.

ARCHITECTURE DU SERVICE I-LIPSO MODE



POINTS D'INTÉGRATION

DIAGRAMME DE SÉQUENCES DU SCÉNARIO :



VI-4 Scénario Prépayé

L'idée est que LIPSO met sur le marché des cartes prépayées reliées à un portefeuille électronique. Pour bénéficier de ce système, un utilisateur de téléphone mobile doit au préalable acheter une carte dans un dépanneur ou chez un marchand de journaux. Il s'agit d'une carte prépayée contenant une somme définie à dépenser 25, 50 ou 100\$ et jetable. Une base de données des marchands – les clients de LIPSO – sera stockée et indexée chez LIPSO de la sorte que chaque client dispose d'un code qui l'identifie de façon unique.

À chaque activation d'une nouvelle carte, le NIP de la carte ainsi que le numéro de téléphone qui a servi à son activation seront stockés dans la base de données. Lors de l'achat, l'utilisateur communique sur son mobile le code du marchand, le produit ou service ainsi que le montant qu'il désire payer.

LIPSO utilise le SMS comme un moyen de vérification de l'identité ; ensuite elle gère la transaction avec son marchand affilié en prélevant une commission du compte électronique du client et en versant le reste de la somme au vendeur.

Un message de confirmation est envoyé du marchand à LIPSO, qui à son tour confirme la transaction à l'utilisateur. L'utilisateur peut réapprovisionner son compte à tout moment en achetant des cartes LIPSO.

Une personne ayant un téléphone mobile et qui achète la carte prépayée LIPSO, se voit créer un portefeuille électronique chez LIPSO. Elle n'a pas besoin de communiquer son nom, ses coordonnées ou son numéro de carte bancaire, seul son code PIN son numéro de téléphone seront ses identifiants.

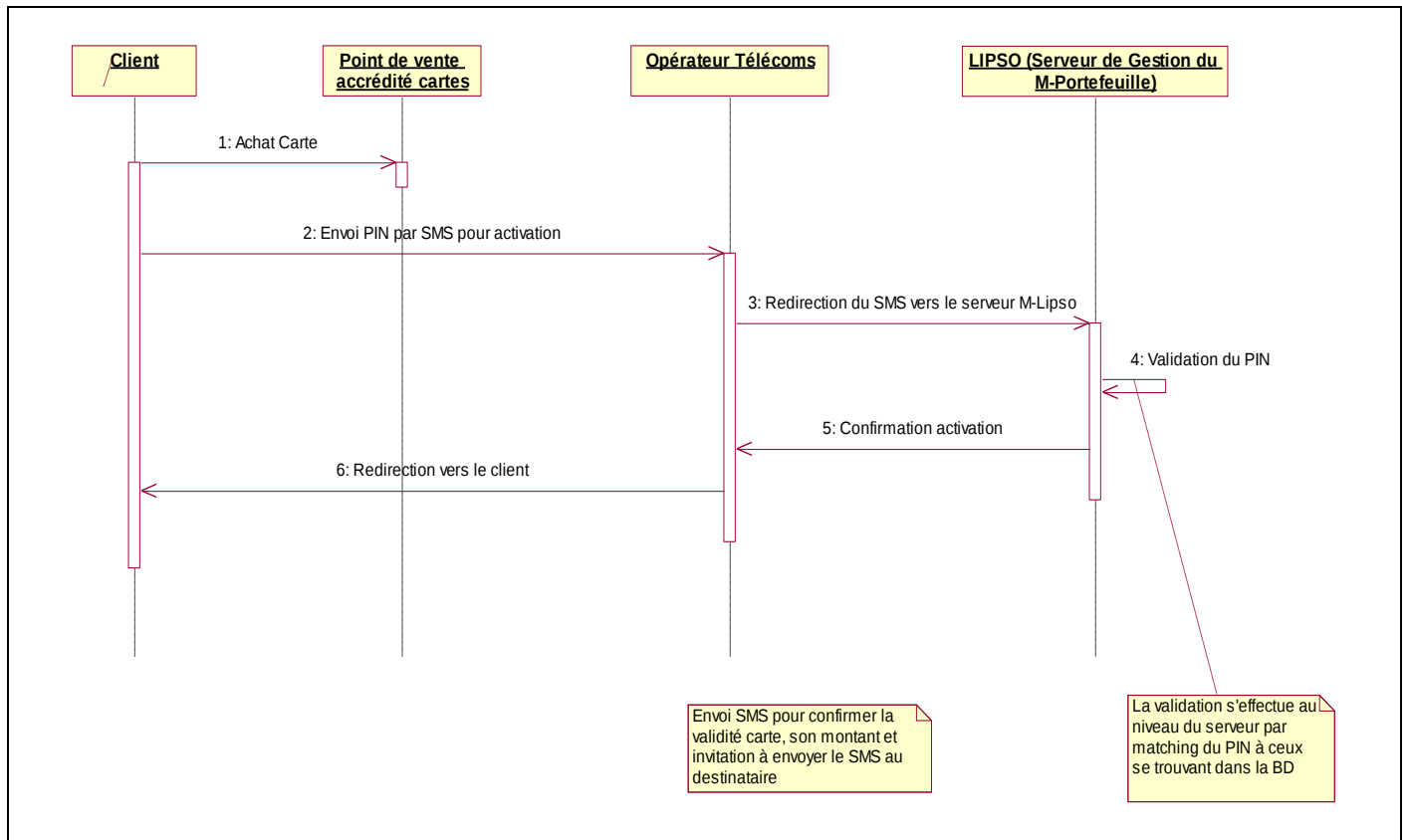
1. Activation d'un nouveau compte

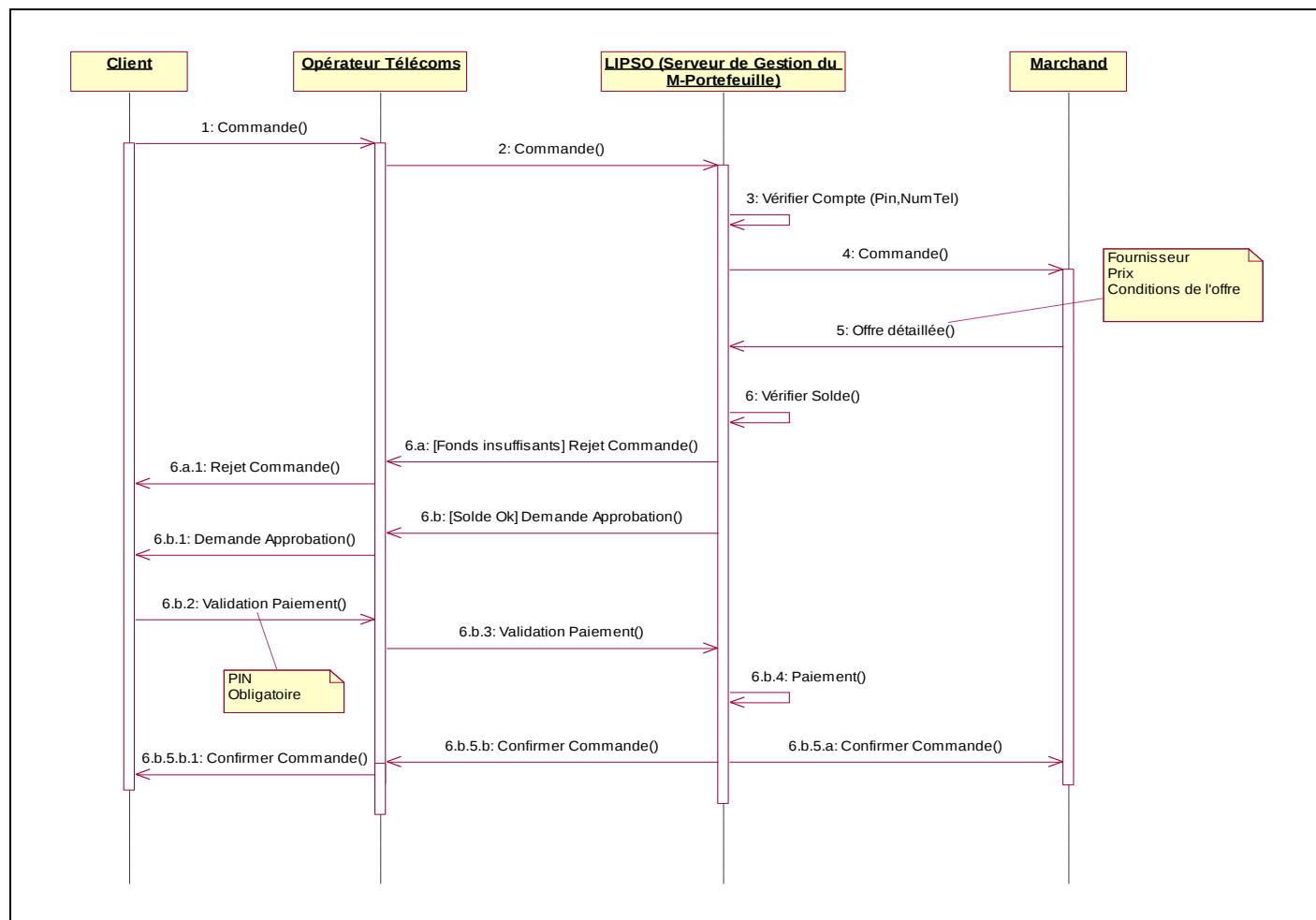
L'activation d'un nouveau compte usager se fait comme suit :

- À l'achat d'une carte, le client envoie un SMS à LIPSO.
- LIPSO vérifie le code NIP avec la base de données des cartes générées.
- Si le NIP est valide, LIPSO crée dans sa base un nouvel enregistrement avec le code PIN de la carte, le numéro de téléphone qui a servi à l'activation ainsi que le montant de la carte :

Numéro de Téléphone	Pin Carte	Crédit
---------------------	-----------	--------

- Un SMS de confirmation est envoyé à l'utilisateur en indiquant le solde de son compte.

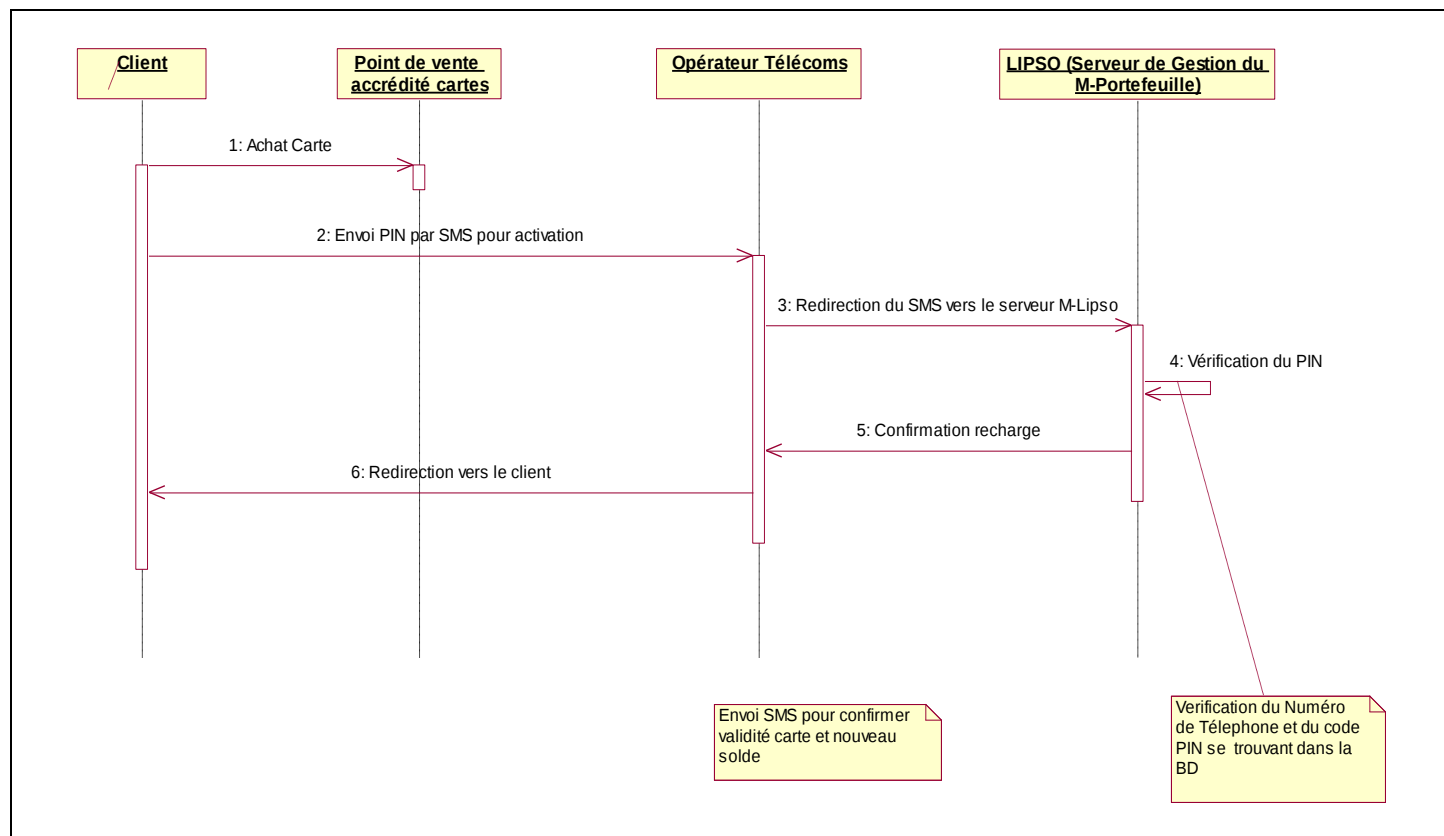
Diagramme de séquences d'activation:



2. Réapprovisionnement d'un compte existant

Dans le cas où un utilisateur désire réapprovisionner son compte :

- Achat d'une carte LIPSO.
- Envoi d'un SMS à LIPSO avec le code PIN de la nouvelle carte.
- Le serveur LIPSO vérifie si ce Numéro de téléphone existe déjà parmi ses clients actifs.
- Si Oui, LIPSO ajoute le montant de la carte au solde actuel du compte.
- Si Non, création d'un nouveau compte.
- Un message SMS est envoyé à l'utilisateur confirmant la transaction ainsi que le nouveau solde.



3. Aspects sécuritaires

Une solution qui permettra de renforcer la sécurité et de réduire le risque de fraude consiste dans le fait que lors de l'activation d'un nouveau compte, le PIN de la carte ainsi que le numéro de téléphone de l'utilisateur sont stockés chez LIPSO. À chaque transaction, LIPSO envoie au numéro de téléphone correspondant au PIN de la carte utilisée un code généré automatiquement et à utilisation unique. Ce code servira de clé pour la transaction. Ainsi, une carte active ne pourra être utilisée que par le téléphone qui a servi à son activation uniquement.

4. Avantages et inconvénients

- Utilisation simple et intuitive;
- Accès à du contenu payant sans engagement;
- Pas de frein psychologique au paiement on-line;
- Paiement même si non bancarisé (adolescents);
- Accélérer la vente de contenu via SMS;
- Paiement non répudiable.

Tout d'abord il faut préciser qu'il existe deux approches d'utilisation de cartes prépayées :

La première consisterait pour LIPSO à détenir uniquement une base de données contenant la liste des numéros PIN. Cette méthode est celle utilisée pour les cartes d'appels interurbains. Son principal avantage est de permettre aux clients de transiger anonymement, cependant de part ce fait, en cas de fraude, il serait plus compliqué pour LIPSO de repérer le fraudeur, même si le numéro de téléphone d'où a été émis la transaction pourrait constituer une piste.

La deuxième approche consisterait pour LIPSO à conserver une base de données contenant les informations des clients abonnés ou inscrits à M- LIPSO, ainsi ces clients auraient un compte chez LIPSO et les cartes ne serviraient uniquement qu'à recharger ce compte. Ce système s'apparente plus aux cartes de recharge Fido. Cette méthode s'avère donc plus sécuritaire puisque les clients sont inscrits et identifiables en cas de fraude.

La prochaine question à se poser est de savoir si dans cette optique l'utilisation de carte prépayée est la meilleure option, pourquoi ne pas recharger son compte LIPSO sur Internet par exemple ? Le principal avantage de l'utilisation de carte prépayée qui serait vendue dans tous les bureaux de poste par exemple est la vulgarisation de la solution. Pour que la solution ait du succès, elle doit être utilisée par le plus grand nombre de personnes possibles et donc cibler une clientèle de masse. Ce n'est pas tout le monde qui a accès à l'Internet et il y a encore moins de personnes qui sont prêtes à se connecter régulièrement sur Internet pour recharger leur compte en LIPSO ; sans compter ceux qui sont réticents à entrer leurs numéros de carte de crédit sur Internet. Certains n'ont tout simplement pas de cartes de crédit. Cependant rien n'empêcherait qu'il y ai plusieurs moyens de recharger son compte LIPSO, on pourrait avoir la possibilité de le faire en ligne mais si l'on veut tenir compte du contexte actuel et mettre en place une solution qui pourrait fonctionner à présent, la carte prépayée semble être la méthode la plus simple et la plus accessible pour tous. Elle permet également à LIPSO d'avoir un nombre minimal de partenaires et d'avoir un contrôle quasi total sur le processus en ce qui à trait notamment à la sécurité et à la facturation. Ainsi cette méthode permet à LIPSO d'opérer sans tenir compte des banques ou des opérateurs téléphoniques, ainsi la solution ne risque pas d'être restreinte aux clients de certaines banques ou de certains opérateurs téléphoniques comme c'est souvent le cas.

Un autre avantage de cette méthode est le fait qu'une fois que le client achète sa carte, tout le reste du processus est effectué par SMS, ainsi LIPSO reste dans son domaine et continue de se concentrer sur les activités qui font sa force.

Enfin, avec le prépayé, LIPSO commence d'abord par recevoir l'argent avant d'offrir le service, cela est donc un avantage pour la compagnie notamment dans la mesure où le risque de ne pas être payé par un client pour le service offert est quasiment nul.

L'inconvénient est que certains clients pourraient être réticents à acheter une carte de 50 ou 100\$ au cas où ils utiliseraient leur téléphone pour une transaction à venir. Ainsi avec un système par carte de crédit ou facturé par l'opérateur téléphonique le client aurait un délai d'un à deux mois avant de régler les frais d'une transaction effectuée ce qui pourrait être une incitation à la consommation. On peut citer aussi dans le cadre des inconvénients de cette solution la possibilité de mémorisation des SMS et ceci peut causer le dévoilement du code PIN. L'association du compte LIPSO avec le numéro du cellulaire à elle même cause un problème de commodité si on est en présence d'une personne qui détienne plusieurs cellulaires, à ce moment là, cette même personne se verra attribuer autant de comptes LIPSO que de numéros de cellulaires (ce qui complexifie la gestion des comptes d'une seule personne au niveau de LIPSO, mais aussi la manipulation fastidieuse générée pour cette personne.)

On constate donc qu'il reste des points à définir, cependant étant donné que LIPSO est une petite compagnie, il serait intéressant d'avoir un système simple, sur lequel elle a un certain contrôle et qui soit le moins risqué possible. Le scénario de carte prépayée correspond donc totalement à ces exigences, il s'agit surtout d'une méthode qui tient compte uniquement du contexte actuel et donc faisable dans l'immédiat. Les deux derniers scénarios se présentent comme des solutions concurrentes d'un point de vue organisationnel. Toutefois, dans une perspective fonctionnelle, ces deux scénarios sont complémentaires et se voient d'être intégrés dans une même solution. Le scénario du prépayé à court terme et le scénario bancaire à moyen et long terme.

LIPSO a tranché dans le choix du scénario final et sur lequel le prototype sera développé. En effet, le scénario du prépayé a été retenue par LIPSO. La section qui suit présente une étude plus détaillée sur la chaîne de valeur du prépayé. Le cahier de charges du prototype est annexé à ce rapport, il constitue l'élément de départ pour développer le prototype.

VII- LE PRÉPAYÉ EN DÉTAIL

Les cartes prépayées représentent actuellement, l'un des plus excitants développements et secteurs de croissance élevée sur le marché⁴. Les solutions prépayées comprennent une sélection encore plus vaste de services dont l'accès à l'Internet, les paris sur Internet, la télé en «pay-per-view» et les alphapages. Ces solutions représentent une source de revenu importante comme le montrent les données suivantes⁵ :

Le marché européen des cartes prépayées a été en 1995 de 1,25 milliards de US\$ (source Eurodata) soit environ 1% du marché de la téléphonie. Une estimation globale basée sur la croissance affichée par les principaux fournisseurs laisse penser que celui-ci a au moins doublé en 1997.

- Le marché total américain des cartes prépayées était en 1990 de 100 000 cartes et il est passé en 1996 à plus de 200 millions de cartes.
- France Télécom a vendu en 1997, 115 millions de cartes à puces dont près de 2 millions de cartes France Télécom. Depuis le lancement du produit, France Télécom a vendu 850 millions de télécartes et il y a près 2,5 millions de cartes France Télécom en service.
- Selon l'EMC corporation, voici les données actuelles et projetées (en millions) concernant les utilisateurs du service prépayé dans le monde entier 2001 – 2004⁶ :

Region	2001	2002	2003	2004
EMEA	258,1	320,9	375,6	427,6
Asia Pacific	27,7	40,7	55,4	71,3
Greater China	55,4	93,4	119,2	156,8
North America	12,5	15,7	18,4	20,3
South America	63,2	86,1	109,7	133
Worldwide	416,2	556,8	678,3	809

⁴ <http://www.nitecrest-fr.com/tapc.htm>

⁵ <http://www.art-telecom.fr/publications/cartel/cartel1.htm>

⁶ <http://www.emc-database.com/>



Ces données expliquent sans doute l'une des raisons pour laquelle LIPSO ait opté pour cette solution dans le cadre du développement du M-portefeuille. La solution du M-portefeuille est basée sur une gestion de cartes prépayées.

L'objectif de cette section est de traiter l'aspect de la mise en marché, la logistique et tous les dispositifs mis en place dans le scénario prépayé. Cette description inclut l'identification des composantes (humaine, système, interface, etc.) des intervenants (imprimeur, distributeur, LIPSO, sous-traitant, client, etc.), description des impacts des décisions et actions prises par les intervenants et description des processus d'affaires tout en considérant les contraintes du marché, coûts, sécurité.

Ce document est composé de cinq parties :

- Le processus d'achat;
- La politique de retour;
- Les relations d'affaires avec les marchands et distributeurs;
- La gestion des fraudes;
- L'impression et distribution.

VII-1 Processus d'achat

Le client se présente chez un bureau de poste, dépanneur ou bien un distributeur et il demande l'achat d'une carte prépayée. Afin d'accéder au service, le client gratte sa carte pour prendre connaissance du NIP et l'envoi à LIPSO par SMS. L'application installée au niveau de LIPSO vérifie le NIP et crée un nouveau compte client (si c'est la première fois). Un délai de 24h est alloué à l'activation du compte. Après 24h, le client reçoit un message SMS de bienvenue lui indiquant son solde courant.

LIPSO envoie à ses clients un catalogue sur lequel figure la liste des marchands qui font affaire avec LIPSO. Le catalogue comporte une liste de marchands groupés par secteur d'activité (santé, alimentation, divertissement, etc.). LIPSO assigne à chaque marchand un code de 4 caractères alphanumériques (un caractère alphabétique et trois chiffres.) Les codes des marchands sont disponibles dans le catalogue LIPSO (version papier et électronique Web.) LIPSO peut aussi offrir un service SMS de recherche par mot clé. Cette recherche constituera une valeur ajoutée pour le SMS transactionnel. En tapant «007#*mot-clé*», l'utilisateur pourra recevoir le code correspondant à ce marchand. Tout ceci pour faciliter la tâche pour la clientèle. Une transaction est enclenchée, lorsque le client envoie un message SMS comportant le code du marchand. Suite à ce message, il reçoit une réponse SMS qui comporte la liste des produits et services disponibles. À chaque produit correspond un code.



Le client envoie le message SMS suivant: «**NIP Usager#Code du produit#Quantité**». Le client reçoit un message d'informations comportant le solde courant de son compte et le numéro de confirmation de la transaction effectuée. Toutefois, le test de disponibilité du service ou produit doit précéder la confirmation du client. LIPSO effectue le transfert des fonds dans le compte marchand.

VII-2 Politique de retour

LIPSO offre une garantie de satisfaction lors des achats de service, si le client n'est pas entièrement satisfait de ses achats, il a la possibilité de retourner ses achats et recevoir un remboursement s'il est admissible. Pour savoir les conditions d'admissibilité et si son retour est éligible, le client vérifie les termes et conditions de LIPSO. LIPSO est responsable de communiquer les termes et conditions clairement à travers le Web ou bien par le biais du centre d'appel. Le client est responsable de prendre connaissance de cette politique. En cas de besoin, le client a la possibilité de communiquer avec le centre d'appel en composant le numéro 1-800 figurant sur la carte afin d'avoir plus d'informations. Le client a aussi la possibilité de communiquer avec le centre d'appel par courrier électronique (support@lipso.com.) Le client n'a pas la possibilité de retourner sa carte et de recevoir un remboursement, si son compte a été activé correctement.

Si le client n'a pas encore gratté la carte, il a encore la possibilité de retourner la carte au distributeur à qui il a fait affaire lors de l'achat de la carte. Le client doit fournir au distributeur la carte munie de la facture d'achat dans les 30 jours qui suivent la date de l'achat. La carte doit être dans son état d'origine et estimée en bonne condition afin de pouvoir la retourner et recevoir un remboursement.

La politique de retour LIPSO s'applique lorsque le client envoie un message SMS d'activation et ne voit pas son compte activé après 24h, le client a reçu un message SMS de bienvenue dans lequel le solde de son compte est incorrect ou bien un problème technique est survenu et qui a affecté la mise en marche du service SMS plus d'une heure (puisque LIPSO garantit 20 min comme maximum d'interruption de service.) Dans ces cas, le client a la possibilité de commencer la démarche de retour soit à travers le Web, la poste ou bien le centre d'appel.



Le client accède à la page de demande de retour et remboursement au site Web de LIPSO. Il entre les informations suivantes :

- Nom;
- Prénom;
- Numéro de téléphone;
- Adresse postale;
- NIP de la carte;
- Nom du distributeur;
- Code du distributeur;
- Description de la raison de retour;
- Date;
- (Signature).

Après avoir terminé l'entrée des données, le client appuie sur le bouton d'envoi et le système assigne un numéro unique à cette demande. Un agent du centre d'appel reçoit la demande, vérifie l'authenticité des informations et communique avec le client par téléphone.

- Si le client désire un nouveau compte, l'agent met à jour le compte client en lui assignant un nouveau NIP, active le compte et annule l'ancien NIP (mettre l'ancien NIP dans la base de données des NIP annulés.)
- Si le client désire recevoir un remboursement, l'agent enlève le NIP du compte client, désactive le compte, annule le NIP et envoie au client un chèque de remboursement à son adresse postale portant le montant initial de la carte. L'opération de la soumission de la demande pourra aussi se faire à travers l'appel au centre d'appel de LIPSO ou bien en imprimant la demande et l'envoyer à LIPSO par voie postale.

VII-3 Relations d'affaires avec marchands et distributeurs

Le scénario des cartes prépayées implique le choix par LIPSO d'un réseau de distribution des cartes. Ces cartes pourraient être disponibles dans les bureaux de poste, les dépanneurs ou les pharmacies. Pour ce faire, LIPSO doit entrer en contact avec ces derniers et établir des ententes afin qu'ils acceptent de vendre les cartes LIPSO. Ces ententes impliquent la discussion sur le montant que LIPSO désire vendre ses cartes aux distributeurs, mais également dans le cadre des grands distributeurs tels que Couche-tard ou les pharmacies Jean-Coutu entre autres. L'entente inclut un montant que LIPSO devra verser à ces derniers pour qu'ils

acceptent de vendre les cartes LIPSO. Compte tenu du caractère confidentiel de ce type d'information, il est difficile d'évaluer ces montants. Cependant, ceux-ci varient selon les distributeurs et les produits, ils sont le fruit de négociations et un même distributeur proposera des montants différents pour plusieurs émetteurs de cartes prépayées. Toutefois, en étudiant le marché actuel, on constate que les cartes prépayées sont vendues aux distributeurs entre 70% et 80% du prix auquel elles seront vendues aux clients. Ainsi, chez FIDO une carte de 10\$ est vendue à 8\$ aux distributeurs, tandis que dans le milieu des cartes à gratter pour les appels interurbains, une carte de 5\$ est vendue autour de 3,50\$. Étant donné la nature des cartes que LIPSO désire mettre sur le marché, il semble judicieux de penser qu'en moyenne, une carte de 50\$ devrait être vendue à 40\$ aux distributeurs. Les montants supplémentaires à payer aux grands distributeurs pourraient être évités comme c'est le cas des cartes de recharge FIDO.

Il s'agit ainsi d'un facteur dont il faut tenir compte dans la mesure où l'accessibilité du produit en dépend. Il faut aussi tenir compte des coûts importants qui ont découlé. À titre d'exemple, depuis plus de six mois les cartes prépayées de TELUS mobilité ne sont pas vendues dans les dépanneurs Couche-tard. La raison est que les deux parties n'arrivaient pas à trouver un compromis sur le montant de l'entente. Pour l'instant c'est le statut quo, chaque partie attend que l'autre cède. Cependant, TELUS est un peu dos au mur, dans la mesure où les montants proposés sont trop élevés pour que les cartes restent rentables. Mais le fait que les cartes ne soient pas distribuées partout se révèle être un sérieux handicap pour la compagnie.

Il s'agit là de l'exemple parfait du type de situation que LIPSO devrait éviter, dans la mesure où il s'agit d'une petite entreprise, le pouvoir de négociation est donc restreint, il serait donc important que LIPSO effectue une analyse de ces coûts de distribution ainsi que des contacts dont elle dispose à l'heure actuelle avant de se lancer dans cette aventure.

Une fois l'entente réalisée, le distributeur commande à LIPSO un certain nombre de cartes. Selon les distributeurs, LIPSO est payée suite à cette commande ou les cartes sont mises en vente dans le magasin et LIPSO n'est payée qu'après que les cartes seraient vendues. Généralement il s'agit de petites commandes (dix cartes par exemple) pour s'assurer qu'elles seront toutes écoulées afin de ne pas avoir à gérer des retours d'inventus.

Nous constatons donc qu'au niveau des relations d'affaires avec les marchands et les distributeurs en ce qui a trait aux cartes prépayées, le succès dépend du pouvoir de négociation. LIPSO doit démontrer au distributeur que c'est lui qui perdrait s'il est le seul à ne pas proposer à ses clients les cartes prépayées LIPSO. Les débuts sont donc critiques, puisque tout deviendra beaucoup plus simple pour LIPSO lorsque le produit sera connu et utilisé par une clientèle de masse.

VII-4 Sécurité et gestion des fraudes

Des niveaux adéquats d'authentification sont essentiels pour garantir véritablement la sécurité du portefeuille mobile virtuel M-LIPSO. L'authentification suppose une combinaison de facteurs qui identifient et légitiment un usager. Il s'agit là d'offrir une authentification comportant deux facteurs : l'identité de la personne est confirmée et son consentement à l'achat est affirmé. Dans le cas de M-LIPSO, ces facteurs comprennent le NIP et une carte à mémoire dotée d'un code unique pour chaque usager.

En effet, tout facteur d'identification d'usager fournit à lui seul un bas niveau d'authentification. À deux, ils offrent un haut niveau d'authentification. Ainsi, une fois l'authentification terminée, la transaction peut être autorisée. Deux options s'offrent à LIPSO pour l'authentification de la demande de transaction provenant d'appareil mobile via :

- Identification d'abonné (cellulaires existants sur le marché);
- Mécanismes de cryptographie tels que signatures numériques ou protocoles de sécurité comme le Wireless Transport Layer Security (WTLS).

La transaction est accomplie entre LIPSO et les marchands et également comporte des protocoles sécurisés de paiement via des protocoles Secure Sockets Layer/Transport Layer Security (SSL/TLS) ou bien des protocoles plus complexe tel que SET7. Ainsi, dans les deux cas, LIPSO joue le rôle d'un serveur de portefeuille., situé au milieu du chemin entre l'appareil mobile et le marchand. M-LIPSO satisfait les exigences des protocoles SSL et SET pour sécuriser la transmission des données en ligne. Il bénéficie également des outils cryptographiques et de processus élaborés qui lui permettent d'offrir une solution de bout en bout à deux facteurs d'authentification.

Notre recommandation est que M-LIPSO soit doté du nouveau standard de chiffrement des données AES8 et une architecture client serveur. Ainsi, M-LIPSO remplit toutes les conditions inhérentes à la non répudiation des transactions mobiles. Il authentifie les parties à la transaction et obtient à la fois le consentement de l'acheteur et l'autorisation de I-LIPSO. Parallèlement, il assure l'intégrité des transactions virtuelles, préserve la confidentialité, et laisse une piste de vérification claire.

⁷ Protocole sûr pour les transactions sur Internet développé par VISA, MasterCard, American Express, etc. C'est ce protocole qui semble devenir aujourd'hui le standard reconnu.

⁸ Nouveau standard de cryptage symétrique, remplaçant le vieux DES (Data Encryption Standard, norme de chiffrement de données). Travaille avec des clefs de 128, 192 et 256 bits. Un algorithme de chiffrement par blocs où il y a une séparation du texte clair en blocs d'une longueur fixe selon un alphabet, et un algorithme chiffre un bloc à la fois. Travaille avec des clefs de 128, 192 et 256 bits.

Cette vérification est faite par le système de vérification M-LIPSO qui contrôle les activités du système, de l'application et du réseau afin de reconstituer en entier n'importe quelle transaction, assurant ainsi la non répudiation des transactions. Il est impossible de divulguer les renseignements recueillis par ce système, à moins que le client n'en fasse la demande expresse.

Quant à la fraude, la solution consiste à identifier les distributeurs par des codes. LIPSO communique à chacun de ses distributeurs des codes sur des tickets collants (stickers.) Le distributeur colle ce ticket, comportant son code, sur chaque carte vendue. L'acheteur compose le PIN de la carte et le code du distributeur et l'envoie par SMS à LIPSO. LIPSO vérifie dans sa base de données l'authenticité du PIN de la carte et le code du distributeur correspondant. Dans la base de données LIPSO, chaque PIN de carte correspond à un, et un seul code de distributeur. Par contre, un code distributeur correspond à plusieurs PIN de cartes. Si toutes les informations sont correctes, LIPSO active le compte client sinon LIPSO a la possibilité de tracer le fraudeur à partir de son numéro de téléphone.

Une carte activée, la première fois, sera désactivée au niveau de la base de données des nouvelles cartes non utilisées chez LIPSO. Dans le cas où une personne essaiera de réactiver une carte déjà active, LIPSO vérifie si le numéro de téléphone correspond bien à celui qui a été utilisé lors de la première activation de la carte :

- Si oui, Un SMS est envoyé par LIPSO indiquant à la personne que son compte est déjà crédité du montant de cette carte en lui fournissant la date de la première activation.
- Sinon, LIPSO informe l'utilisateur par SMS que la carte est déjà activée par une autre personne et qu'en cas de litige, l'utilisateur doit contacter le centre d'appel par téléphone. Le numéro du service à la clientèle sera fourni à travers un message SMS.

Dans le cas où cette personne appelle le centre d'appel, deux scénarios sont envisageables :

- S'il y a des doutes à propos de la crédibilité de l'appelant, le préposé avise l'appelant des conséquences que peut engendrer une tentative de fraude. Le préposé recueille les informations personnelles de l'appelant (nom, prénom, adresse) et l'avise qu'une enquête sera tenue dans les 24 heures qui suivent et qu'il se verra crédité son compte dans les délais.
- Si le préposé trouve que la personne est assez crédible, il vérifie d'abord si c'est un nouveau client ou un ancien :

- Si c'est un nouveau, il récolte les informations personnelles de l'appelant et l'avise qu'il sera contacté par SMS dans les prochaines 24 heures.
 - Sinon, le compte est crédité du montant de la carte et bloqué jusqu'à la fin de l'enquête.
- Dans tous les cas, le préposé a le droit, sous justificatifs, de bloquer, créditer ou débiter un compte.

Concernant le centre d'appel qui abrite le service à la clientèle de LIPSO, trois scénarios se présentent :

- LIPSO crée une petite cellule de 5 à 10 personnes qui s'occupe de gérer les appels du service à la clientèle. Cette solution peut être coûteuse pour LIPSO surtout pour un démarrage.
- LIPSO sous-traite son service à la clientèle. Plusieurs centres d'appel offrent leurs services aux PME à Montréal. Je cite entre autres, l'agence JONCAS POSTEXPERTS qui œuvre dans le domaine et actuellement se charge d'une partie de l'activité du service à la clientèle de VIDEOTRON, Journal de Montréal, etc.
- LIPSO intègre la solution «Customer Care Management System» de LOGICA9 qui permet l'accès aux comptes clients à travers le Web.

VII-5 Impression et distribution

La génération des codes devant servir à la conception des cartes prépayées, est effectué au sein de LIPSO grâce à un générateur de codes. Elle s'effectue dans un cadre sécurisé en utilisant des algorithmes de génération de nombres pseudo aléatoires. L'utilisation de tels algorithmes, assure la quasi-impossibilité de trouver des numéros valables. Une fois les codes générés, ils sont chiffrés et sauvegardés sur un support mobile pour être transportés chez l'imprimeur par un opérateur. La sauvegarde de la confidentialité des données est assurée par un échange de clé pour effectuer le chiffrement (chez LIPSO) et le déchiffrement (chez l'imprimeur).

⁹ http://www.logica.com/lmnflash/docs/payments/product_info/pi_customer_care.pdf

Dans le marché de l'impression des cartes prépayées, nous distinguons de nombreux joueurs dont les plus importants sont :

- Bouygues Télécom;
- Oberthur Card systems;
- Keystone;
- GEMPLUS.

Il existe différentes catégories de cartes auxquelles sont associées des normes précises. Ainsi, on distingue des cartes à logique câblée, des cartes à microprocesseur et des cartes à mémoire simple¹⁰. Les cartes à logique câblée et des cartes à microprocesseur sont considérées comme des cartes intelligentes. En effet, ces cartes peuvent être dotées d'une mémoire programmable disposant de fonctions élémentaires d'identification, d'authentification et de sécurité de niveau élevée. Elles sont utilisées comme carte de fidélisation à un commerce, carte bancaire et carte de téléphonie cellulaire de type GSM. Mais dans le cadre de notre étude, nous allons plus en détail nous pencher sur les cartes à mémoire simple.

Les cartes à mémoire simple ne disposent pas de mémoire programmable. Toutefois, elles disposent d'une mémoire dite simple, utilisées sous formes de jetons qui sont décrémentés au fur et à mesure que le titulaire de la carte l'utilise. Dans le cadre du M-Portefeuille, cette mémoire est faite des codes générés couverts par une mince couche de substance à gratter dite zone de "scratch". L'utilisateur doit gratter la substance pour avoir accès à son code pour effectuer l'activation auprès de LIPSO. En plus des cartes simples qui ne peuvent être réutilisées une fois le crédit attaché à la carte terminé, LIPSO a la possibilité de gérer les cartes prépayées rechargeables. De façon précise, LIPSO gère les jetons représentés par les codes inscrits sur la carte. Les caractéristiques principales de la carte à mémoire simple sont les suivantes¹¹ :

- Mémoire à grilles sous forme de jetons;
- Pas d'espace pour inscrire des données en mémoire;
- Pas de protection par code secret;
- Pas de comportement spécifique programmable;
- Pas de système d'exploitation;
- Simple d'utilisation et économique.

¹⁰ Source : Autoroute de l'information, Gouvernement du Québec.

¹¹ Source : Autoroute de l'information : Gouvernement du Québec.



Ces cartes pourront être faites à base de polyester transparent pour assurer la résistance contre les changements extrêmes de température. Elles peuvent aussi être de différentes couleurs avec des motifs faits suivants les clients ciblés.

Les cartes ainsi fabriquées, sont entreposées chez le fabricant après vérification et approbation du produit par LIPSO. La livraison des cartes chez les marchands et les points de ventes se fait de façon mensuelle par une entreprise spécialisée (par exemple sécur.). Toutefois, cette livraison peut se faire à la demande des grands marchands.

La mise en marché dépendra d'un facteur clé, qui est le nombre des marchands participants et des points de vente. Pour ce faire, LIPSO doit nouer des ententes avec des grands noms tels que Postes Canada, les magasins couches-tard, les réseaux de distribution de presse et tabacs, la grande distribution, les grands magasins, les réseaux de franchise et les entreprises de vente par correspondance¹². Bien plus, les cartes prépayées LIPSO pourront être vendues par les opérateurs de services de télécommunication et les distributeurs de télécommunication en marques propriétaire, sous leur propre nom et selon des ententes précises. Une autre possibilité demeure celle de la sous-traitance. Dans tous les cas, la soumission du produit auprès des détaillants pourra se faire selon un modèle de vente à prix réduit (par exemple vendre auprès des marchands participants une carte LIPSO de \$10 à \$8.5.) Ce modèle a pour avantage de ne pas recouvrir à un processus de recouvrement complexe s'étalant sur de longues périodes. L'encaissement par LIPSO des montants auprès des marchands se fait une fois le produit livré.

¹² Observatoire TÉNOR / CESMO des Cartes Téléphoniques Prépayées : www.cesmo.fr



CONCLUSION

La solution du prépayé paraît simple à première vue. Mais, en analysant en détail les infrastructures qu'il faut mettre en place, les ententes et les partenariats stratégiques que LIPSO doit établir et la gestion de la sécurité qui reste un point important à régler avant de mettre en marché la solution, il est clair que cette solution requiert un lourd dispositif.

Il faut aussi noter que le service du SMS transactionnel ne peut réussir que si les habitudes des gens se transforment vers un tel comportement d'achat. Il est vrai que l'étude qu'on a fait ne touche pas ce point. Néanmoins, c'est un début pour une autre étude qui traitera la population ciblée et les marchés porteurs pour un tel service. Une erreur que peut commettre les gens est de transposer les modèles qui ont réussi sur Internet de leur environnement initial vers le monde mobile. Rappelons que c'est la cause derrière l'échec du WAP.

Enfin, plusieurs des obstacles concernant la sécurité sans fil qui se posent aujourd'hui disparaîtront avec l'adoption massive de la technologie de troisième génération. Ces cellulaires seront basés sur l'IP et supporteront plus de capacité de computation, de mémoire et de bande passante. En combinant la technologie 3G avec des cartes prépayées, ou des cartes à puces et de biométrie, les entreprises pourront avoir un système sécurisé unique pour le réseau sans fil.



ANNEXE 1

CAHIER DES CHARGES

M-PORTEFEUILLE : LE PORTEFEUILLE ELECTRONIQUE MOBILE LIPSO

DATE	Le 3 Juin 2003
WORK PACKAGE	Prototype M-Lipso Version 2
NUMÉRO DU DOCUMENT	PROML-02
CLASSIFICATION DU DOCUMENT	Interne
NOM DU FICHIER DU DOCUMENT	cahierChargesMLipso.pdf
INSTITUTION	HEC Montréal/Université de Montréal (Montréal, Québec)

Résumé

Ce document est une version initiale des spécifications de conception du prototype de l'application de portefeuille mobile virtuel M-LIPSO dans le cadre du scénario de paiement par carte prépayée. En tant que tel, ce document ne prétend pas être une version finale de l'application mais plutôt être vu comme un point de départ pour des discussions et des travaux futurs.

I- INTRODUCTION

La création d'un prototype pour le scénario de paiement par carte prépayée M- LIPSO, nous permettra de présenter les fonctions principales que nous souhaitons implémenter, mais aussi d'obtenir des commentaires sur l'interface utilisateur (GUI). Nous le voyons comme un processus incrémental, hautement itératif, représentable par une boucle de rétroaction (feed-back).

Un cahier de charge est un document qui met en relief la spécification des besoins. Notre prototype M-LIPSO, comme tout produit ou logiciel a des spécifications et des besoins à satisfaire. Ces besoins et comment parvenir à mettre en place le prototype vont être détaillées et explicitées tout au long de ce document.

Comme tout mandat qui se voit être digne d'expertise et de professionnalisme, le développement du prototype M- LIPSO respecte la notation UML et le schéma de la base de données - le formalisme entité relation. Le développement du prototype sera décomposé comme suit :

- Besoins de l'application.
- Élaboration du schéma de la base de données et du diagramme de classes.
- Développement des modules java nécessaire à la gestion des différents objets (Usager, Carte, Distributeur, Transaction, Marchand) et l'interrogation de la base de données.
- Développement du module de formatage des fichiers XML.
- Développement du module de communication (envoi des sockets).
- Intégration des différents modules.

II- BESOINS

Partant du constat que nous allons développer un prototype pour le scénario du prépayé et du fait que nous sommes limités par le temps, nous allons définir des besoins qui se veulent cohérents par rapport à ces deux constatations sus indiquées. En outre, nous ne pouvons pas procéder à un test effectif de l'application M-LIPSO auprès d'utilisateurs réels (end-users), ou des utilisateurs indirects afin de jauger l'intérêt pour l'application.

Ainsi, nos besoins s'articulent autour des points suivants :

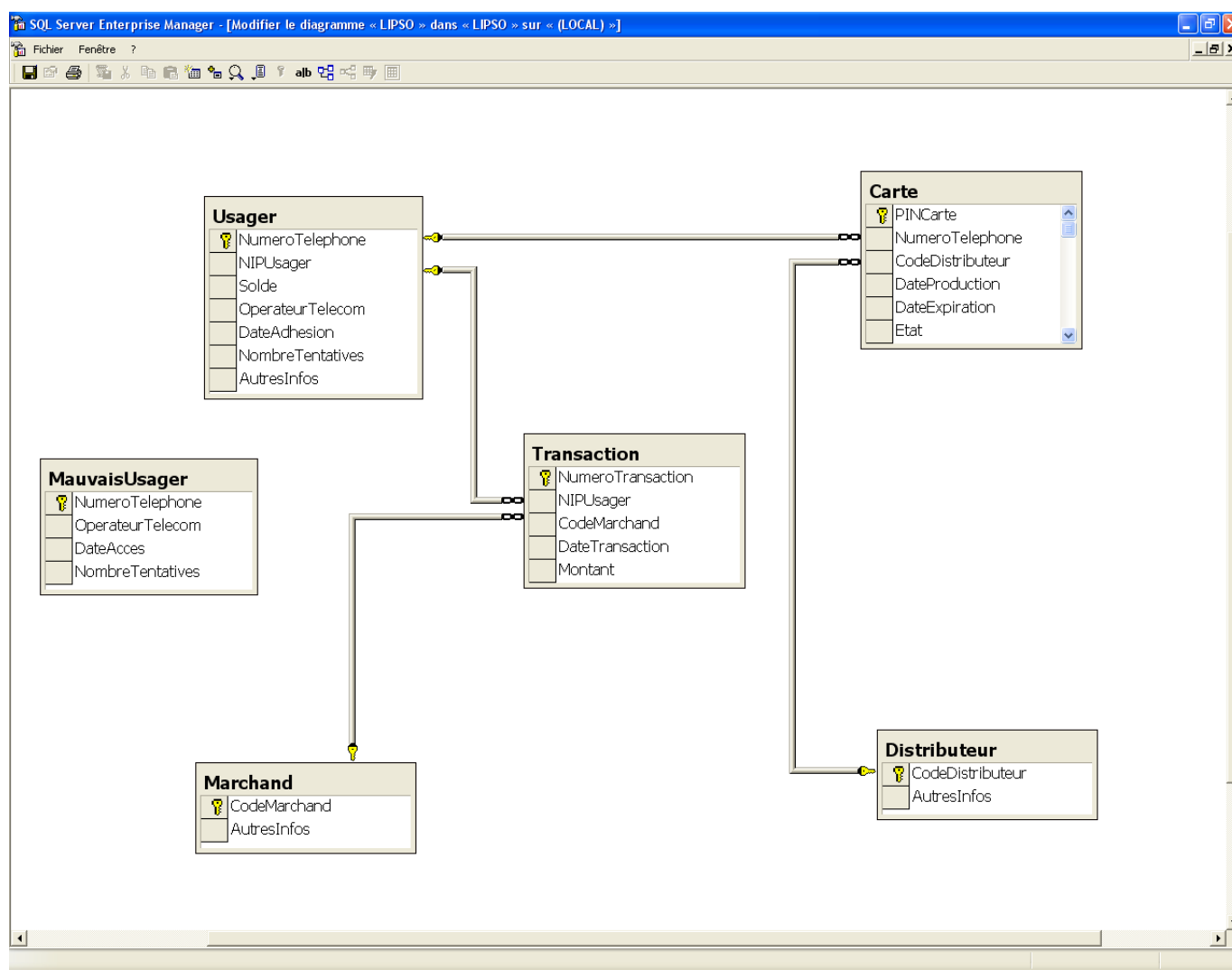
- Génération statique des numéros de cartes.
- Activation des cartes.
- Gestions du cycle de vie des cartes (activée, bloquée, expirée)
- Procédure de transaction.

III- ETAPES DU PROTOTYPAGE

III-1 Structure des données

Pour rendre accessible notre base de données, la première étape à franchir consiste en une description de la structure générale de nos données par l'entremise du schéma de la base de données ci-dessous :

SCHÉMA DE LA BASE DE DONNEES





III-2 Environnement de développement

Le développement se fera en Java dans des machines personnelles. L'intégration quant à elle sera élaborée au niveau de LIPSO. La DTD (Document Type Description) de LIPSO nous a été confié pour le formatage de toutes les communications avec i-LIPSO à travers des documents XML.

III-3 Module de communication

Il s'agit d'un modèle permettant la communication inter processus (IPC - Inter Processus Communication) afin de permettre à divers processus de communiquer aussi bien sur une même machine qu'à travers un réseau TCP/IP.

Nous allons utiliser le mode connecté (comparable à une communication téléphonique), utilisant le protocole TCP/IP. Dans ce mode de communication, une connexion durable est établie entre les deux processus, de telle façon que le Socket de destination n'est pas nécessaire à chaque envoi de données.

1. EXEMPLE DE CODE POUR LA FORMATION DES SOCKETS ET DE LEUR ENVOI

```
import java.io.*;
import java.net.*;

Socket monSocket = new Socket(InetAddress.getByName(adresseIP), port);
BufferedReader monEntree = new BufferedReader(new
InputStreamReader(monSocket.getInputStream()));
PrintWriter maSortie = new PrintWriter(new
OutputStreamWriter(monSocket.getOutputStream()));

maSortie.println(monMessage);
maSortie.flush();
while((line = monEntree.readLine()) != null)
{
System.out.println(line);
}
monEntree.close();
maSortie.close();
monSocket.close();
```



2. EXEMPLE DE CODE POUR LA RÉCEPTION D'UN SOCKET

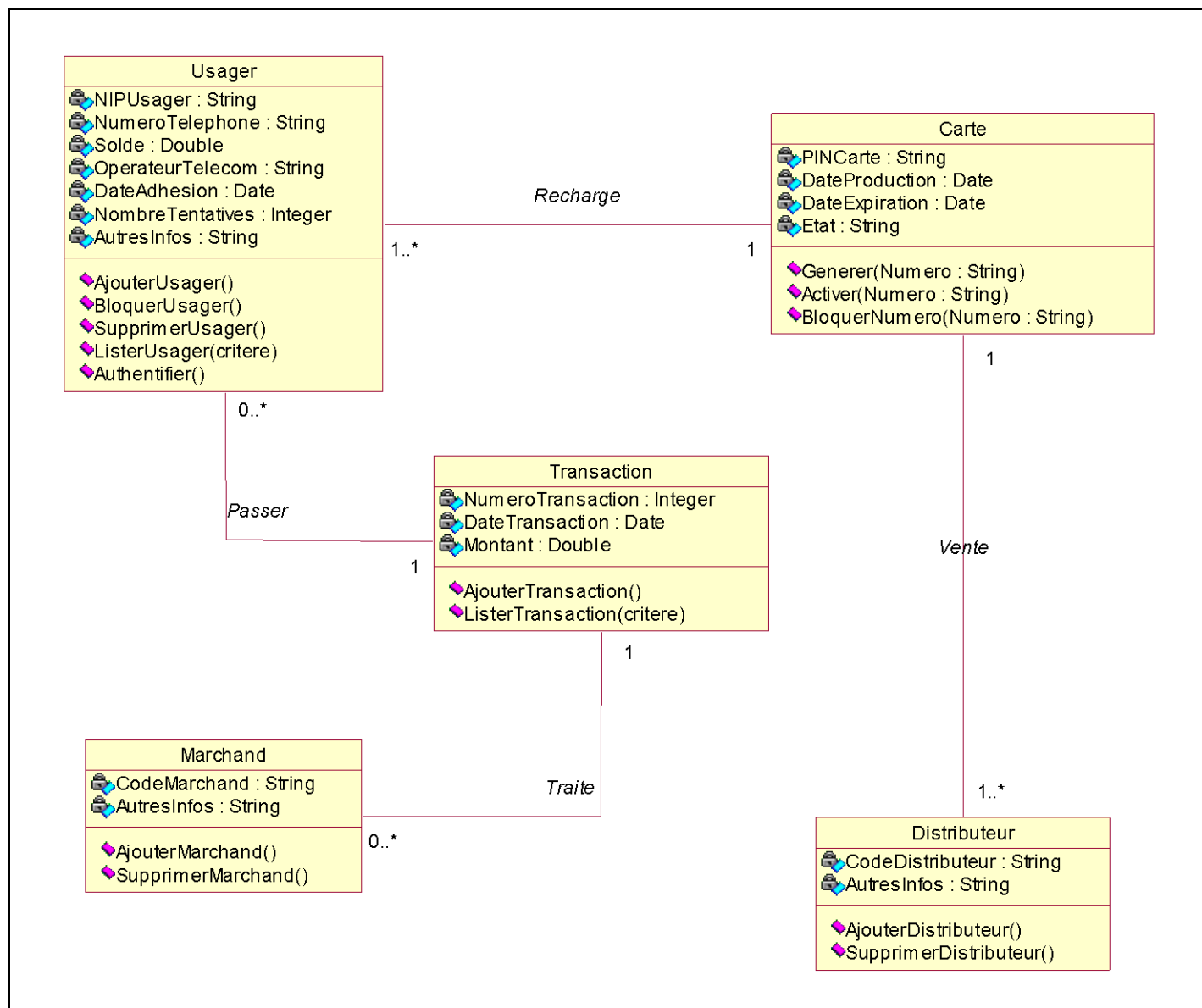
```
import java.io.*;
import java.net.*;

ServerSocket socketServer = new ServerSocket(port);
Socket client = socketServer.accept();
BufferedReader monEntree = new BufferedReader(new
InputStreamReader(client.getInputStream()));
PrintWriter maSortie = new PrintWriter (new
OutputStreamWriter(client.getOutputStream()));

String line = monEntree.readLine();
System.out.println("> Recu: " + line) ;
maSortie.println("Echo: " + line);
maSortie.flush();

monEntree.close();
maSortie.close();
```

III-4 Diagramme de classes



III-5 Scénarios et diagrammes de séquences

1. Cas d'utilisation Activation

i) Description détaillée

Cas d'utilisation #	Activation d'une carte prépayée	
Description	Activation d'une carte de valeur donnée	
Acteur	Client titulaire ou non d'un M-Portefeuille	
Pré conditions	Avoir déjà acheter une carte.	
SCÉNARIO PRINCIPAL	étape	Action
	1	Envoyer un message SMS au serveur LIPSO (# obligatoire) <i>#PIN.</i>
	2	Le système reçoit le message, l'analyse, vérifie la validité du code PIN de la carte dans la BD.
	3	Le code est valide, le système vérifie l'existence d'un compte M-Portefeuille associé au numéro de portable.
	4	Le client est titulaire d'un M-Portefeuille, le système additionne la valeur de la carte au solde du client.
	5	Le système envoie un message SMS au client contenant son nouveau solde et un rappel sur les moyens disponibles pour changer son NIP Usager. <i>Votre nouveau solde est : \$35.75.</i> <i>Pour changer votre NIP Usager appeler le 1-800-444-2003 ou envoyer un SMS : #Ancien NIP Usager#Nouveau NIP Usager</i>
SCÉNARIO SECONDAIRE	étape	Action de branchement
	3	Le code PIN est non valide
	3.a	Le système vérifie si le nombre de tentatives avec échec à partir de ce numéro de portable n'a pas dépassé les 3. Le système vérifie aussi si le nombre global de tentatives avec échec n'a pas dépassé un certain nombre au cours de cette journée (Indice de la présence d'un hacker).
	3.b	Les deux conditions sont vérifiées ou l'une d'elles, le système envoie un message d'erreur. <i>Votre code PIN est invalide</i>



	4	Il n'existe pas de compte M-Portefeuille associé au numéro de portable
	4.a	Le système crée un compte
	4.b	Le système envoie un message SMS au client contenant son nouveau solde. Son NIP Usager et une description sur les moyens disponibles pour changer son NIP Usager. <i>Votre nouveau solde est : \$35.75.</i> <i>Votre NIP Usager est : SMSemaster</i> <i>Pour changer votre NIP Usager appeler le 1-800-444-2003 ou envoyer un SMS : #Ancien NIP Usager#Nouveau NIP Usager</i>
Post conditions		Le système met à jour le solde M-Portefeuille et désactive le code PIN de la carte dans la BD.

2. Cas d'utilisation Transaction

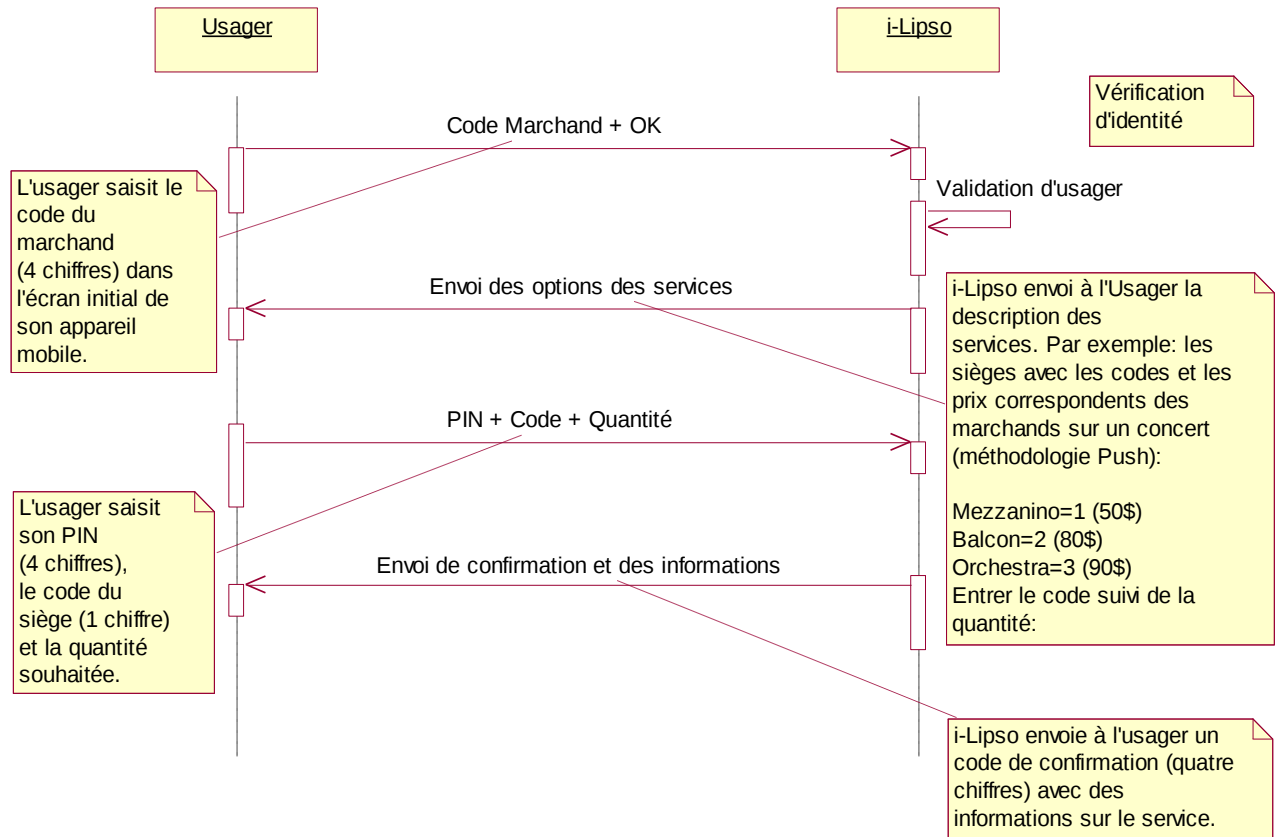
- ii) Description détaillée : Nous proposons un prototype pour l'achat de billet d'un concert organisé par l'entreprise Palmarium. Il existe trois types de sièges ; Mezzanine, Balcon et Orchestre.

Cas d'utilisation #	<i>Transaction pour l'achat d'un billet de concert</i>	
Description	Commander son billet	
Acteur	Client titulaire d'un M-Portefeuille	
Pré conditions	Avoir un M-Portefeuille contenant suffisamment de fond.	
SCÉNARIO PRINCIPAL	étape	Action
	1	Le client envoie un message SMS au serveur LIPSO contenant le code du marchand <i>1616</i>
	2	Le système reçoit le message, l'analyse et vérifie l'existence d'un M-Portefeuille associé au numéro de portable.
	3	Le client est titulaire de M-Portefeuille, le système contacte l'application marchand et prépare l'offre.
	4	Le système retourne un message SMS au client: <i>Concert de Jazz organisé par Palmarium le 17 Juin 2003-06-02</i> <i>Mezzanine = m (\$50)</i> <i>Balcon = b (\$80)</i> <i>Orchestre = o (\$90)</i>



		<i>Entrez votre NIP Usager, le code du siège et la quantité et (exemple : 25689m2):</i>
	5	Le client reçoit le message, appuie sur Reply et saisit son NIP Usager, le code du siège et la quantité.
	6	Le système envoie un message SMS au client contenant son nouveau solde et un rappel sur les moyens disponibles pour changer son NIP Usager. <i>Votre nouveau solde est : \$35.75.</i> <i>Pour changer votre NIP Usager appeler le 1-800-444-2003 ou envoyer un SMS : #Ancien NIP Usager#Nouveau NIP Usager</i>
	7	Le système analyse le message, vérifie le NIP Usager associé au numéro de portable, vérifie que le client a suffisamment de fond pour payer sa commande.
	8	Le système confirme la réservation auprès du marchand, qui lui retourne le ou les numéros de siège.
	9	Le système envoie un message de confirmation au marchand et un message SMS au client contenant son nouveau solde et le numéro de siège. (Le numéro de portable et le numéro de siège seront la preuve d'identité du client lorsqu'il se présente au concert) <i>Votre du numéro de siège au concert je Jazz organisé par Palmarium le 17 juin 2003 est : M84.</i> <i>Votre nouveau solde est \$10.50.</i>
SCÉNARIO SECONDAIRE	étape	Action de branchement
	3	L'utilisateur n'a pas de compte M-Portefeuille.
	3.a	Le système lui retourne un message décrivant la façon de créer un compte M-Portefeuille (voir scénario d'activation), enregistre le numéro de portable dans la BD afin d'éviter de lui répondre une prochaine fois.
	4	Il n'y a plus de places disponibles dans ce concert.
	4.a	Le système envoie un message d'épuisement des billets.
	7	Le NIP Usager est erroné, le système vérifie si le client n'a pas dépassé les trois tentatives avec échec.
	7.a	Le système envoie au client un message d'erreur <i>Votre NIP Usager est erroné: si vous avez oublié votre NIP Usager appeler le service à la clientèle 1-800-444-2003.</i>
Post conditions		Le système met à jour le solde M-Portefeuille.

DIAGRAMME DE SÉQUENCE
SCÉNARIO PRINCIPAL DE LA TRANSACTION M-LIPSO



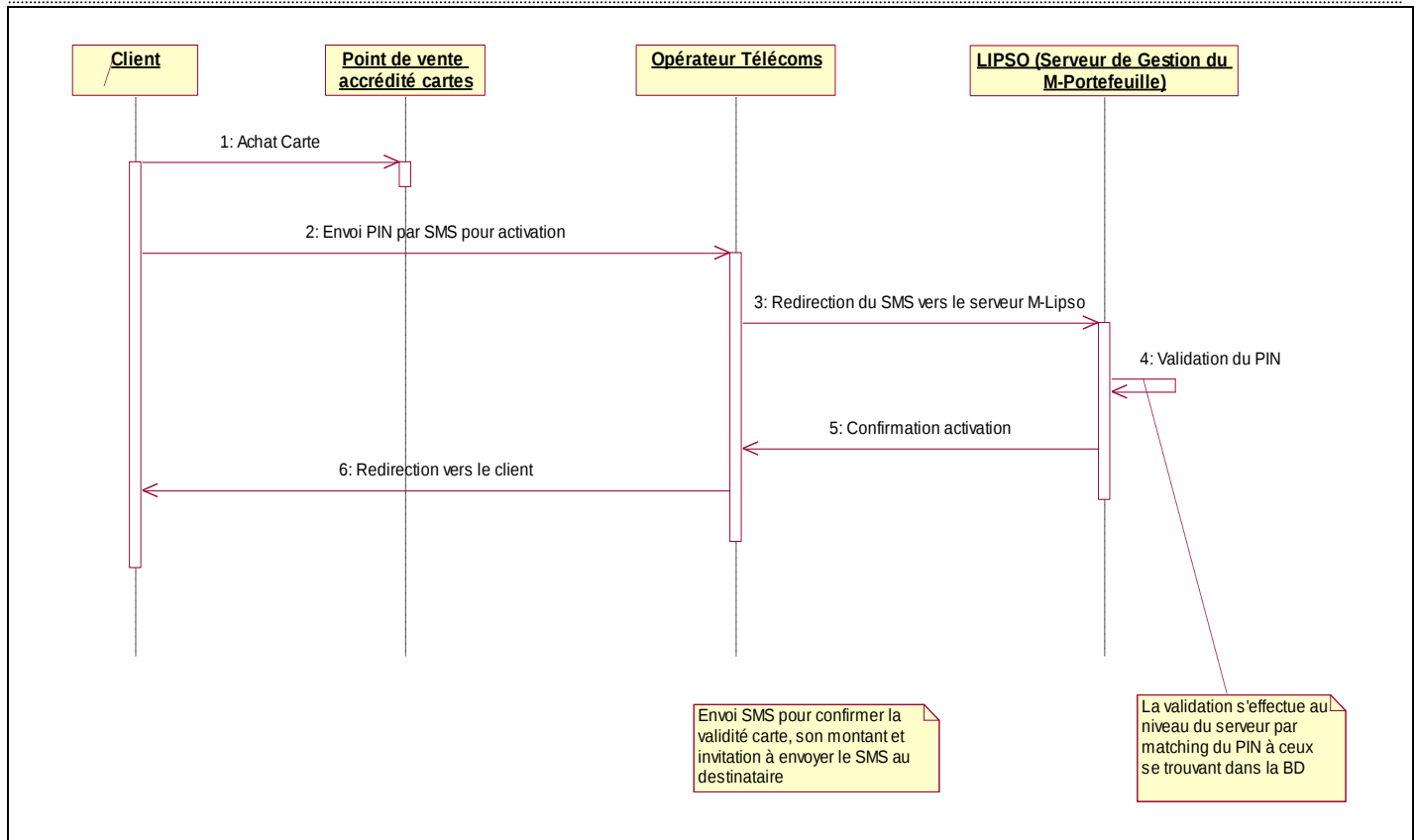
III-6 Gestion des cartes prépayées

1. GÉNÉRATION STATIQUE DES NUMÉROS DE CARTES

Notre prototype simulera la génération des numéros des cartes prépayées. Ainsi, une série de numéros vont être générés aléatoirement et stockés au niveau de la base de données (Table Carte). Dans la solution réelle, tout un mécanisme de génération et de chiffrement des numéros doit être mis en place. Un tel choix est dicté par la contrainte temps.

2. ACTIVATION DES CARTES

Après avoir acheté une carte du distributeur, l'utilisateur a besoin d'alimenter son compte M-LIPSO ou d'en créer un nouveau si c'est la première fois. L'utilisateur n'a qu'à introduire le code PIN de la carte. Un accusé sera envoyé en cas de succès ou d'échec (voir le cas d'utilisation de l'activation 5.1).



3. GESTIONS DU CYCLE DE VIE DES CARTES (ACTIVÉE, BLOQUÉE, EXPIRÉE)

La carte a un cycle de vie bien définie. Elle passe d'un état à l'autre selon où elle se trouve. Chez l'imprimeur, la carte est bloquée. Tandis que chez le distributeur, elle est activée. S'elle dépasse une durée bien définie (6 mois), elle expire. Le tableau qui suit résume les différents états que peut avoir la carte prépayée :

<i>Situation</i>	<i>État</i>
Chez l'imprimeur	bloquée
Entre imprimeur et distributeur	bloquée
Chez le distributeur	activée
Achetée par l'utilisateur et non utilisée	activée
Achetée par l'utilisateur et utilisée	bloquée
La date de commercialisation est dépassée	expirée
Tentatives de fraude détectée	bloquée



Nous pouvons même imaginer une solution plus sécuritaire dans la gestion de cycle de vie des cartes prépayées. Cette solution consisterait à relier les différents distributeurs de ces cartes au serveur central de LIPSO. Tout achat ou retour de carte sera comptabilisé en ligne. Ainsi, une personne qui devine un numéro de carte ne pourra bénéficier de l'argent de ce numéro que si le distributeur qui a reçu la carte informe le serveur LIPSO de l'achat effectif de la carte. De ce fait, une carte ne passera à l'état activée que si l'acheteur et le distributeur envoient un signal au serveur pour l'activer. Le premier par le biais d'un message SMS et le deuxième à travers le réseau IP.

IV- SÉCURITÉ

L'objectif de cette section est de relever les différences en terme de sécurité entre l'envoi d'un message SMS à partir d'un site Web (en utilisant des passerelles) et son envoi à partir d'un téléphone mobile.

IV-1 Site WEB (Public gateways)

- Anonymat de l'utilisateur (pas de l'adresse IP) : l'utilisateur pourra envoyer un message SMS à partir de n'importe quel ordinateur.
- Renseignements personnels : la possibilité de faire la consultation des SMS envoyés dans le cas de litige (logiciel spécifique qui offre cette fonctionnalité¹³).
- Un désavantage de l'utilisation de public gateways est la sécurité des fichiers. Au contraire des transmissions Web qui surviennent comme des transactions sécurisées, quelque tierce partie pourra surveiller le téléphone mobile et le contenu du message envoyée à travers un public gateway. Les messages envoyés à partir du téléphone mobile pour les centres Short Message Service sont plus sécurisées, mais il y a toujours la possibilité que ces transmissions puissent aussi être surveillées.

IV-2 Téléphone Mobile

- Pas d'anonymat puisque l'utilisateur pourra être tracé par le numéro de son téléphone mobile (couplé dans certains cas avec son nom), ou par sa carte SIM (Subscriber Identity Module) intégrée dans l'appareil.
- L'appareil mobile est limité en comparaison avec des équipements typiques de sécurité qui peuvent être installés sur une machine (PC).

¹³ SMStoB : <http://smstob.com/?par=google>



- Les usagers de téléphones mobiles deviennent de plus en plus vulnérables à une foule d'attaques précédemment adressées plutôt à l'Internet. Ils sont de plus en plus connectés, donc plus susceptibles à des menaces d'attaques. Ainsi, la prolifération (SMS/MMS-Multimedia Messaging Services) amène à un taux d'infection plus considérable.
- Fonctionnalités de Lycos¹⁴ : Code de sécurité présente au moment de son inscription et de l'envoi de son SMS à recopier.
- L'utilisation croissante du roaming¹⁵ de la part des usagers de téléphones mobiles, rend impossible de filtrer et localiser les messages nuisants. Les attaques via SMS existent déjà depuis quelques temps, mais jusqu'ici la majorité des instruments utilisés avec les SMS étaient des SMS bombers, une attaque très faible de la part des amateurs.
- Les personnes ne peuvent pas faire confiance à ce qui semble avoir été envoyé par quelqu'un, s'elles ne sont pas en mesure de vérifier d'une façon fiable l'authenticité de l'expéditeur. Cependant, Nokia a développé deux modèles tels que 9110 et 9210, utilisant les systèmes SMS de signature numérique. Nki Security Messenger est un outil qui nous permet d'envoyer des SMS cryptés à travers un téléphone Nokia en préservant les renseignements personnels de nos messages SMS, ainsi seulement les vrais destinataires pourront les lire. NkiSecurityMessenger est basé sur une technologie de chiffrement connue comme 128 bit forte encryption pour le code ASCII, Rijndael AES algorithme de chiffrement par bloc pour Unicode.
- Le SIM (Subscriber Identity Module) intégré dans le téléphone mobile, offre aujourd'hui des caractéristiques de sécurité qui sont plus souples et plus efficaces

¹⁴ Lycos: <http://www.linternaute.com/mobile/sms/smsgratuits1.shtml>

¹⁵ Roaming: Se déplacer d'une couverture d'Access Point (AP) vers une autre couverture d'AP sans perdre sa connexion.

¹⁶ ASCII Text File / PGP Armored Encrypted File

V- ARCHITECTURE DU PROTOTYPE

Le développement du prototype a passé par les étapes suivantes :

- Compréhension de la DTD de LIPSO.
- Formatage des messages à transmettre en fichiers XML (respect de la DTD LIPSO).
- Finalisation des contrôles (les différentes requêtes vers la base de données).
- Envoi des messages via des sockets.
- Réception des sockets et leur décomposition pour ressortir les messages.

Notre Prototype met en jeu deux modules développés en Java et bénéficiant de la programmation concurrente. Le premier module est celui de communication, le deuxième est de contrôle (Voir Figure).

V-1 Module de communication

Ce module a pour objectif de :

- Réception des sockets provenant à une adresse IP et un port bien spécifiques;
- Envoi des sockets;
- Extraction des informations du fichier XML qui a été reçu à travers le socket;
- Envoi des informations vers le module de contrôle;
- Réception des informations du module de contrôle;
- Formation des fichiers XML avec les informations reçues du module de contrôle.

V-2 Module de contrôle

Ce module a pour objectif de :

- Réception des informations du module de communication;
- Vérification syntaxique des informations reçues;
- Interrogation de la base de données;
- Envoi des informations au module de communication suite aux réponses de la base de données.

Nous décomposons notre traitement en deux. L'activation de la carte et la transaction. Lors de l'activation de la carte, le module de contrôle a besoin de recevoir du module de communication les informations suivantes :

- Téléphone Usager;
- PIN carte;
- Code distributeur.

Après contrôle, le module de communication recevra un message contenant le solde de l'utilisateur, et le cas où il y a un problème, une erreur sera envoyée (PIN Carte erroné, Code distributeur incorrect). La transaction quant à elle sera décomposée en deux étapes. Lors de la première étape, le module de communication enverra les informations suivantes au module de contrôle :

- Téléphone Usager;
- Code marchand.

Durant deuxième étape, le module de communication enverra les informations suivantes au module de contrôle :

- NIP Usager;
- Code produit;
- Quantité.

