Titre: Title:	Système électronique de transport, transfert et d'échange numérique de valeurs
Auteur: Author:	Octavian Urèche
Date:	1999
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Urèche, O. (1999). Système électronique de transport, transfert et d'échange numérique de valeurs [Thèse de doctorat, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/8874/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/8874/
Directeurs de recherche: Advisors:	Réjean Plamondon
Programme: Program:	Non spécifié

UNIVERSITÉ DE MONTRÉAL

SYSTÈME ÉLECTRONIQUE DE TRANSPORT, TRANSFERT ET D'ÉCHANGE NUMÉRIQUE DE VALEURS

Octavian URECHE

DÉPARTEMENT DE GÉNIE ÉLECTRIQUE ET DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION
DU DIPLÔME DE PHILOSOPHIÆ DOCTOR (Ph.D.)
(GÉNIE ÉLECTRIQUE)

SEPTEMBRE 1999

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée:

SYSTÈME ÉLECTRONIQUE DE TRANSPORT, TRANSFERT ET D'ÉCHANGE NUMÉRIQUE DE VALEURS

présentée par: URECHE Octavian

en vue de l'obtention du diplôme de: Philosophiæ Doctor

a été dûment acceptée par le jury d'examen constitué de:

M. LEFEBVRE Louis A., Ph.D., président

M. PLAMONDON Réjean, Ph.D., membre et directeur de recherche

M. PIERRE Samuel, Ph.D., membre

M. CHERIET Mohamed, Ph.D., membre externe

*À mon père **Vasile** et à ma mère **Gabriela Lydia***

mais surtout

*À ma grand-mère **Carolina***

REMERCIEMENTS

Je désire avant tout remercier mon directeur de recherche, le professeur ***Réjean Plamondon***, pour avoir montré sa confiance en moi et en ce projet depuis le tout début et de m'avoir guidé et soutenu moralement tout au long de mes études post-universitaires. Son support moral constant et sa patience inébranlable m'ont été indispensables pour la réalisation de cet ouvrage.

Je tiens également à remercier tous mes collègues du **Laboratoire SCRIBENS** qui m'ont offert un environnement de recherche passionnant et dynamique. Je tiens à souligner ici la collaboration très utile de ***Wacef Guerfali***, ***Hong Trang Nguyen***, ***Shahram Moïn***, ***Salim Djeziri***, ***Sylvia Sabeva*** et ***Alessando Zimmer***. Je n'oublie pas non plus la collaboration d'***Hélène Dallaire*** et je tiens à la remercier pour son aide ponctuelle et éclairée.

Enfin, je remercie tout particulièrement ***Carl Desjardins*** pour la relecture du manuscrit qui a précédé cet ouvrage et pour ses commentaires intéressants et ses suggestions précieuses. Ses idées m'ont aidé à éclaircir davantage certaines explications et m'ont permis ainsi d'augmenter la qualité de ce travail.

RÉSUMÉ

Le travail de recherche présenté dans cet ouvrage s'inscrit dans le contexte général du commerce électronique et plus particulièrement dans le contexte de la sécurité des transferts de données et des transactions sur les réseaux de communications numériques ouverts. Concrètement, notre travail porte sur plusieurs aspects transactionnels et monétiques de l'économie numérique et touche de près les notions reliées aux transactions – et en particulier aux paiements – numériques sur Internet.

Afin de bien amorcer notre travail et pour cibler correctement les éventuels manques et besoins dans ce domaine, nous avons commencé nos recherches avec une étude bibliographique des moyens de paiement sur Internet. Tout d'abord, nous avons introduit une nouvelle taxonomie, assortie d'une liste de critères d'analyse et d'évaluation qui nous ont permis de réaliser une première revue quasi exhaustive des systèmes électroniques de paiement sur Internet. Ce survol des systèmes de paiement électronique nous a permis de voir quelles sont leurs caractéristiques principales, leurs avantages et désavantages respectifs et de démontrer le besoin à combler par un nouveau système de transfert de valeurs.

Nous avons ainsi proposé les bases d'un nouveau système transactionnel qui capitalise sur plusieurs points forts de certains systèmes existants et minimise, voire élimine, certains de leurs inconvénients respectifs, tout en apportant des solutions originales à plusieurs niveaux du design. Pour ce faire, nous avons introduit un nouveau concept transactionnel qui vise à généraliser plusieurs notions décrites dans la recherche bibliographique.

Nous avons ainsi introduit le concept d'***instrument unifié de transport, de transfert et d'échange de valeurs numériques***, permettant de transiger plus que des fonds – même si ce type de transfert constitue l'application de base du nouveau système – et qui donne une totale flexibilité aux usagers à plusieurs niveaux du design. Le système informatique que nous introduisons, baptisé TRANZIX, est un nouvel outil transactionnel, généralisant la notion de paiement, tant du point de vue du contenu, que du point de vue des opérations.

Premièrement, TRANZIX généralise le contenu d'un paiement permettant ainsi de transférer ou transiger tout objet virtuel ou réel qui peut être numérisé et avoir une représentation binaire. Ces objets peuvent être soit des billets virtuels ou des certificats binaires, soit des attestations électroniques, des pièces d'identification ou tout autre document numérique.

En même temps, TRANZIX généralise l'opération de paiement, pour prendre le sens plus large de transaction. Ainsi, une valeur peut être ***transportée*** de l'endroit A à l'endroit B sans que cette valeur ne change de propriétaire. Elle peut aussi être ***transférée*** de B à C, non seulement en changeant d'endroit – par transport –, mais en changeant aussi de propriétaire. Enfin, elle peut être ***échangée*** avec d'autres valeurs, la notion d'échange impliquant deux transferts lors d'une même transaction.

TRANZIX emploie le concept d'***enveloppes virtuelles*** comme moyen de transfert de valeurs et repose sur un protocole de transport des enveloppes virtuelles (PTEV) pour le transport proprement dit. Les billets virtuels sont une première application du système; ces billets auront une valeur marchande, étant payés d'avance. Le système emploie des ***billets numériques personnalisés*** à l'aide de moyens biométriques – par exemple, les signatures manuscrites des usagers. Le système assure un niveau de sécurité très élevé, employant un algorithme de chiffrement asymétrique, et offre une granularité arbitrairement ajustable, permettant ainsi d'intégrer le concept de ***micropaiements***.

Le système est ***direct*** – donc n'utilise pas d'intermédiaires lors du transfert de valeur –, ***symétrique*** et exclusivement logiciel donc ni l'entité client ni l'entité serveur n'ont à acheter des équipements matériels dédiés, et de plus, chacun peut utiliser le même logiciel autant pour vendre que pour acheter. L'équipement matériel n'est utilisé que par l'émetteur.

À ce jour, TRANZIX est le premier ***système intégré mixte***, ou bimodal, qui offre le choix entre des transactions en-ligne et hors-ligne. Dans le premier cas, le système contacte pour chaque transaction l'émetteur ou le certificateur de la valeur en question – approche utile pour les transactions importantes. Dans le mode hors-ligne, le système permet un lien direct entre un acheteur et un vendeur, sans contacter un tiers – approche utile pour les transactions à faible valeur. Le système offre aussi aux usagers le choix de la modalité de communication (TCP/IP, SMTP, de façon «non-électronique» – à l'aide d'une disquette, par exemple) entre les entités transactionnelles. L'utilisation d'une telle approche pourra faciliter l'intégration du système dans une architecture intranet, permettant d'effectuer des transactions entre les différents départements d'une entreprise.

Un exemple intéressant d'application du système TRANZIX concerne les ***transactions mixtes***, ou concurrentes, dans lesquelles différents types de valeurs sont échangés lors d'une même transaction. Un cas typique d'une telle transaction est constitué par l'échange de documents électroniques accompagnés d'un ou plusieurs billets virtuels, servant de paiement.

Employant le PTEV, TRANZIX offre la possibilité à toutes les entités transactionnelles d'utiliser leurs portefeuilles virtuels respectifs pour transiger de manière facile et directe tout objet virtuel, permettant ainsi l'intégration des outils d'échange de documents électroniques et des outils de paiement numérique dans un seul instrument transactionnel. D'autres applications peuvent inclure l'échange et la présentation électronique de valeurs (cartes d'identité, pièces justificatives, etc.), la facturation de différents types (à l'utilisation, inter et intra-départementale dans une compagnie, micro-achats à distance, etc.) ou le contrôle d'accès (à l'aide de jetons numériques) à des ressources internes ou externes, virtuelles ou physiques.

ABSTRACT

The research project presented in this thesis analyses various aspects of the new digital economy in the context of secure data transfer and digital transaction handling over open communication networks. Specifically, our work deals with several monetary and transactional issues related to the general concept of electronic commerce, and in particular, to the notion of electronic transactions over the Internet.

We start off by introducing a few basic notions and general definitions and we present several concrete means of securely transporting documents on public communication networks. Different approaches are shown in a comprehensive survey of digital payment systems for Internet-based electronic commerce. A new taxonomy and classification covering most, if not all, Internet payment methods, schemes and protocols is introduced. A set of evaluation and analysis criteria, both internal and external to a particular system, is used to analyze system representatives of each class. The principal characteristics are summarized in a comparative table.

Based on this analysis, a list of needs and requirements for a flexible new system is determined. We introduce the general notion of generic «***transfer of value***», achieved by using ***digital envelopes***. In this context, we propose a new transactional

concept based on a ***digital envelope transfer protocol*** (DTEP), used for ***transport, transfer and exchange of value***, irrespective of what they actually might represent. We define ***transport*** as the process of conveying any virtual object – such as an electronic document (e-document), digital bill or token, etc. – from point A to point B, either by copying it or by moving it, without losing or changing its ownership. ***Transfer***, in addition to moving the virtual object, implies a change of ownership. Finally, an ***exchange*** implies two transfers, in both directions, as part of the same transaction.

The new protocol allows digital transactions to be independent of the intrinsic nature of the payload; any binary files with a non-intrinsic value could represent monetary and non-monetary values to be negotiated digitally: funds, tokens, coupons, credentials and any other documents that can be in any way represented in a digital manner could form a payload and could be transported, transferred or otherwise exchanged using the DETP. In this manner, electronic transactions become substantially more flexible. Based on this protocol, a new system, named TRANZIX, allows different types of electronic documents or other digital valuables to be transported and exchanged concurrently using the same support.

The system provides a very high level of security, protecting data contained in its digital envelopes through public-key-based encryption. Encryption is also used to limit and control accessibility to the system, while user authentication and data integrity are secured using digital signatures. Authentication is complemented by additional biometric protection based on handwritten signatures, which also ensures non-repudiation. The same biometric methods are also used for the offline part of the protocol in order to prohibit double-spending.

TRANZIX offers a short collection delay for e-shops and its digital bills provide reasonable anonymity that could accommodate both individuals and governments. The system is also symmetric, both buyers and vendors can use the same

software-only virtual wallet to transact, transport or transfer any digitizable object having a non-intrinsic value, including, in particular, money. As a software-based solution that does not involve costly hardware investments, TRANZIX can keep installation and maintenance costs down.

While other systems employ digital cash to achieve funds transfer, TRANZIX uses digital bills to complement the payload as payment for the service. Virtual cash is therefore only one among many different kinds of e-documents that can take advantage of this transactional system. Electronic documents to be transported, transferred or exchanged can be obtained or rendered in a standardized format through a certification issuer who signs them and certifies their accuracy. The certification issuer can be the user himself, provided that his signature will be trusted and valued enough by his transactional counterparts. In the case of financial transactions, digital bills can be bought from an issuing bank using any «real world» means available – cash, check, money order, credit card, etc.

A prototype of this system has been implemented in Java and can be used for micropayment billing. As microtransactions could generate a huge overhead, TRANZIX can reduce this drastically by offering offline payment and verification options. Depending on the amounts involved, merchants can reduce their costs by verifying the bills they receive, in batch mode, at the end of the day. In our opinion, this allows substantial reductions, both in overhead and costs, making micropayments economically viable.

Two sorts of objects can be handled by TRANZIX. One comprises virtual or digital objects, i.e. electronic representations of digitized documents, credentials, IDs, certificates, and so on. The other comprises physical objects, i.e. physical resources such as computing power, intranet peripherals (scanners, printers, speakers, etc.), physical access to specified premises (doors, locks, etc.), and so on. To control access to

such objects, as well as the manner in which they are handled, TRANZIX employs digital tokens, centrally distributed to intranet or extranet users. Each token serves as a certified credential granting limited access to a predetermined object. Tokens are standardized and easily customizable to serve designated collections of objects with specific access details such as the time of use, the duration of use, the amount of resources available and allowable, and so on.

Several targeted applications are presented, including the controlled access to physical resources on an intranet using tokenized micropayments, as well as the customized retailing of virtual objects and other digital resources on the Web. Another useful application presented involves ***mixed transactions***, transactions in which several e-documents and other virtual objects – such as digital cash or electronic certificates – are exchanged concurrently as part of the same exchange or purchase. In such transactions, a document can be exchanged for another document in addition to one or more digital bills that serve as payment. Employing the DETP, TRANZIX allows all entities to use their respective virtual wallets to transfer all transactional elements, in an easy and straightforward manner. This helps integrate document exchange and financial transfer tools in one single transactional instrument. Different approaches for future developments are proposed. A comprehensive list of electronic resources is also included.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

LISTE DES ABRÉVIATIONS

CGI	*Common Gateway Interface*
DFD	Diagramme de Flux de Données
DH	Diagramme Hiérarchique
EDI	Échange de Documents Informatisés
E/S	Entrées/Sorties
FDA	*Food ans Drug Administration*
HTML	*HyperText Markup Language*
HTTP	*HyperText Transfer Protocol*
ID-biométrique	Identificateur biométrique
IP	*Internet Protocol*
JIT	*Just in Time*
MHz	Mégahertz
NIP	Numéro d'Identification Personnel
OBI	*Open Buying on the Internet*
OCDE	Organisation de coopération et de développement économique
PME	Petite et Moyenne Entreprise
PTEV	Protocole de Transfert d'Enveloppes Virtuelles

RM	Représentation Monétaire
ROM	*Read Only Memory*
SET	*Secure Electronic Transaction*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UID	*User Identification*
URL	*Uniform Resource Locator*
US	*United States [of America]*

CHAPITRE 1

INTRODUCTION

Les années 90 nous ont plongés à grande vitesse dans un nouveau médium de communication, donnant ainsi un avant-goût du prochain millénaire. Les industries de l'information dominent aujourd'hui l'économie; les estimations de la valeur du marché des informations électroniques en-ligne varient entre 10 et 100 milliards de dollars US par année – tout dépendant de quelle façon ce marché est défini. Des dizaines de milliers de bases de données sont accessibles sur les différents réseaux électroniques de communications, des produits informationnels allant des logiciels informatiques complexes, valant plusieurs milliers de dollars, aux journaux électroniques ou cotations boursières valant quelques cents chacune. La croissance fulgurante des ventes en-ligne reflète la vitesse à laquelle cette nouvelle économie électronique s'accroît.

Depuis quelques années déjà, plusieurs réseaux électroniques de communications, aussi bien publics que privés, se sont regroupés dans une grande confédération internationale de réseaux, connue sous le nom d'Internet. Ce réseau est à l'heure actuelle le plus connu, le plus accessible et transporte la plus grande quantité d'information, parmi tous les autres réseaux informatiques publics ou privés.

L'Internet, ce réseau mondial de communications numériques, connaît aujourd'hui une croissance explosive: plus de 100 millions d'usagers dans plus de 150 pays, et un million de nouveaux utilisateurs qui s'y joignent chaque mois. Son importance est reconnue tant par les marchés financiers que par les gouvernements de tous les pays développés, à travers le monde.

Initié en 1969 par le **Département Américain de la Défense**, la colonne vertébrale de l'Internet (terme appelé communément «*backbone*») entre en 1986 sous la juridiction de la **National Science Foundation** (**NSF**) qui la gère jusqu'en 1995 [Raran, 1995]. Avec l'accroissement du nombre d'usagers, un pourcentage de plus en plus grand du trafic appartient au secteur commercial.

Deux événements majeurs ont déterminé le virage commercial de l'Internet. Premièrement, le retrait des subventions du gouvernement américain, fournies à la **NSF** pour l'administration de la colonne vertébrale, au début de 1995, a ramené la majorité des réseaux qui composent l'Internet sous contrôle privé et donc en quête de nouveaux clients pour supporter les coûts. Par ailleurs, l'introduction au début des années 1990 d'un nouveau service, le *World Wide Web* (Web), disposant à partir de 1993 d'une interface graphique possédant des fonctionnalités multimédia, a permis en quelque sorte la vulgarisation des technologies de communication informatiques. Cette nouvelle interface non seulement introduit des nouvelles applications, mais englobe aussi tous les anciens services offerts sur l'Internet, dans un environnement facile et intuitif à utiliser: les communications électroniques ne sont plus réservées aux spécialistes du domaine ou au personnel académique, mais sont désormais accessibles à tout le monde. Ce super-réseau, permet aujourd'hui plusieurs types de transfert d'information, privé, publique ou commercial, mais, à une condition: le transfert, quel qu'il soit, doit être numérique. Le potentiel commercial de ce nouveau médium de communication devient de plus en plus grand: en servant de marché commercial, l'Internet est en train de changer de façon dramatique les habitudes des consommateurs.

Cette explosion de popularité qui entoure aujourd'hui les communications numériques, en particulier le réseau Internet, offre d'inestimables opportunités de développement et de croissance sur plusieurs plans: technologique, éducationnel, économique et social; à cet égard, un nouveau concept, celui du ***commerce électronique*** a été introduit récemment pour définir un des secteurs ayant un des taux de croissance les plus élevés. Ce nouveau concept a eu à son tour une évolution fulgurante dans la deuxième moitié de la dernière décennie, faisant ressortir rapidement l'aspect économique de ce nouveau monde virtuel: la nécessité d'effectuer des transactions numériques, dans un environnement en constante évolution à des vitesses sans précédent. Ces changements ont déjà eu et auront de plus en plus d'effets à tous les niveaux de la vie économique, ainsi qu'à tous les niveaux de la société [Porat, 1977]. Mais le simple transfert de fonds et les ordres de paiement se sont avérés insuffisants comme instruments transactionnels, pour bien compléter les outils multimédia déjà existants, servant au transport d'informations.

En effet, d'autres types de transfert d'information sont essentiels au développement économique du nouveau monde virtuel. Partout où se fait sentir le besoin de communiquer de façon sécuritaire et confidentielle, d'identifier et d'authentifier le correspondant qui se trouve à l'autre bout de la ligne, un support différent est nécessaire, en plus des instruments permettant les transferts de fonds en-ligne. Avec un tel support, n'importe quelle donnée binaire ou document électronique pourrait être transféré en toute quiétude sur un réseau numérique de communication – tout en gardant les fonctionnalités requises pour le transfert numérique de fonds –, ouvrant ainsi de nouvelles opportunités d'échange et d'affaires, tant aux particuliers qu'aux entreprises.

D'autres façons de communiquer, directement, sans toujours passer par un point central, sont aujourd'hui de plus en plus utiles et nécessaires, dans un environnement en croissance permanente et en congestion régulière, où les gens

cherchent un maximum de flexibilité et de liberté de choix. Ainsi, dans un nouveau protocole ayant une telle flexibilité, le rôle de source ou de destination de tout transfert numérique d'information – données brutes, informations, documents électroniques, fonds – pourrait être assumé par n'importe quel utilisateur, à sa guise. Ceci offrirait la possibilité à tous et chacun de chercher, d'acquérir ou d'offrir, à l'aide de transactions numériques, une variété incalculable d'informations, de produits ou de services. Cette diversification des produits et services offerts sur Internet monte déjà à mesure que la popularité de ce nouveau médium s'accroît et que de nouveaux supports transactionnels font leur apparition. Le raffinement de la valeur de cette offre commence à s'accroître à son tour, faisant ressortir le besoin de transiger de montants de plus en plus infimes.

C'est pour répondre à ces besoins, entre autres, que nous avons amorcé le projet qui a engendré comme résultat principal cet ouvrage. Nous avons ainsi introduit le concept d'***instrument unifié de transport, de transfert et d'échange de valeurs numériques***, permettant de transiger plus que des fonds – même si ce type de transfert constitue une application de base du nouveau système – et qui donne une très grande flexibilité aux usagers, à plusieurs niveaux du design – par exemple, au niveau de la manière de communiquer, en-ligne ou hors-ligne.

Un autre aspect primordial des transactions numériques est lié à la confiance des utilisateurs – élément absolument nécessaire, mais pas nécessairement suffisant pour assurer le succès d'un système transactionnel. La sécurité des transactions est un des éléments de base sur lequel repose cette confiance. C'est pour cette raison que nous nous intéressons aussi aux méthodes permettant de sécuriser davantage les transactions, en introduisant une nouvelle approche, qui emploie des moyens biométriques de personnalisation, notamment l'image de la signature manuscrite des utilisateurs.

Les recherches effectuées dans le cadre de cet ouvrage se veulent une contribution au développement d'une solution viable, sécuritaire et performante au

problème de transfert numérique de documents électroniques et de fonds virtuels. D'autre part, plusieurs caractéristiques importantes sont regroupées autour d'une même idée directrice – la liberté transactionnelle des utilisateurs – pour créer un nouveau protocole transactionnel sur lequel reposera un nouveau système de transfert de valeurs. D'une autre part, une nouvelle solution de sécurité est introduite afin de renforcer la confiance des usagers, qu'ils soient acheteurs, vendeurs ou banquiers.

Cette thèse comprend sept chapitres. Ainsi, dans le présent chapitre présentons brièvement la thèse, sa raison d'être et la méthode de travail employée. Le deuxième chapitre nous permettra de regarder de plus près les transactions numériques sur des réseaux publiques de communication. Tout d'abord, nous allons faire une mise en situation, en présentant la croissance rapide des communications, surtout numériques, et du besoin économique d'échanger électroniquement. Nous continuerons en introduisant la problématique, le besoin et les défis du commerce électronique en général et des transactions numériques sur des réseaux publiques en particulier.

Suite à la présentation de plusieurs définitions et généralités concernant les concepts de base, les acteurs et les différentes modalités de paiement, nous allons introduire une taxonomie ainsi qu'un ensemble de critères d'évaluation et d'analyse nous permettant de faire le point sur l'état de l'art dans les paiements numériques. Pour ce faire, nous allons présenter les résultats d'une vaste revue des principaux systèmes de paiement électronique, en faisant ressortir leurs caractéristiques, leurs avantages et leurs inconvénients. Nous allons appliquer les critères de classification introduits afin de comparer les différents systèmes de paiement électronique existants, ce qui nous permettra de faire ressortir les besoins qu'un nouveau système devrait rencontrer ainsi que les aspects qu'il devrait améliorer.

Ces aspects seront développés dans le chapitre trois, chapitre dans lequel nous allons analyser en détail les besoins d'un nouveau système et proposer une

nouvelle solution au transfert numérique de valeurs. Nous allons présenter brièvement le concept général, les aspects de base sur lesquels nous allons mettre l'accent, ainsi que les limites que nous allons fixer à l'aide de différents choix de design.

Le chapitre quatre présente le cœur de l'ouvrage, le ***système électronique de transfert numérique de valeurs***, TRANZIX. C'est ici que nous introduisons ce nouveau système et le concept de base sur lequel il repose: les ***enveloppes virtuelles***, leur utilité et leur fonctionnement. Les spécifications fonctionnelles du système sont décrites et le diagramme de flux de données est présenté. Nous poursuivons en proposant le design préliminaire, design respectant les besoins des différents intervenants impliqués dans une transaction. Nous allons présenter son diagramme hiérarchique et sa structure de données, en montrant, à différents niveaux d'abstraction, les détails du design.

Par la suite, nous allons concentrer nos efforts sur les moyens d'assurer la sécurité du nouveau système électronique de transfert numérique de valeurs. Nous allons regarder les sources potentielles d'erreur et de fraude, ainsi que les instruments qui nous permettent de les éliminer. Ainsi, nous présenterons les moyens employés par le système TRANZIX pour assurer le traitement des exceptions – erreurs, pannes ou fraudes –, de sécurisation par des moyens cryptographiques et de personnalisation par des moyens biométriques.

Nous présentons au chapitre cinq une brève étude des performances de TRANZIX en se basant sur un prototype expérimental que nous avons implanté. Nous avons utilisé ce prototype pour simuler le comportement du système complet, afin d'effectuer une première évaluation de ses performances, en fonction des principales contraintes de design. Nous discuterons ainsi des résultats obtenus expérimentalement, tels que les temps de génération des clés cryptographiques et les temps de transaction.

Dans le chapitre six, nous discutons de l'impact socio-économique, des avantages potentiels et des contraintes éventuelles qu'un système comme TRANZIX pourrait avoir pour le commerce électronique en général et pour les différents intervenants en particulier. Nous allons voir brièvement comment TRANZIX et d'autres systèmes semblables pourraient influencer certains aspects de l'économie et de la société dans le futur. Des scénarios différents sont présentés, suivant le modèle d'émission à adopter et le type de couverture de la représentation monétaire émise. Les questions de l'anonymat des transferts et de l'infrastructure à utiliser seront aussi abordées. Nous discuterons enfin quelques initiatives gouvernementales dans le domaine législatif.

Enfin, le septième et dernier chapitre est dédié aux conclusions, nous permettant de faire le point sur ce que nous avons accompli dans cet ouvrage et de proposer des futures directions de développement. Ainsi, nous résumons ce que notre travail a apporté de nouveau, tout en présentant brièvement quelques améliorations possibles du système et du protocole. Finalement, nous jetons un bref regard vers les nouvelles avenues de recherche envisageables. Une vaste liste de ressources numériques et de pointeurs vers d'autres informations en format électronique qui complètent cet ouvrage, ainsi qu'une démonstration simulée des applications déjà implantées, seront inclus dans la bibliographie et en annexe, respectivement.

CHAPITRE 2

LES TRANSACTIONS NUMÉRIQUES SUR DES RÉSEAUX ÉLECTRONIQUES DE COMMUNICATIONS

Ce deuxième chapitre se propose d'effectuer une incursion sommaire dans le monde des paiements numériques qui utilisent comme support de transmission les réseaux publics de communication numérique. Ainsi, nous nous proposons d'une part, de définir la problématique des méthodes électroniques de paiement et, d'autre part, d'effectuer une revue en profondeur de l'état de l'art du domaine afin de bien situer le cadre et les directions de notre recherche.

Dans un premier temps, une mise en situation sera effectuée, suivie de l'introduction de plusieurs définitions et notions générales qui seront utilisées tout ou long de cet ouvrage. Dans un second temps, nous allons introduire une nouvelle taxonomie reliée aux systèmes de paiement sur Internet, ainsi qu'une série de critères d'analyse et d'évaluation de ces systèmes.

Ces deux outils nous aideront à effectuer une revue quasi complète des principaux systèmes de paiement électronique sur Internet, à évaluer et à analyser leurs caractéristiques, leurs avantages et leurs inconvénients. De cette façon, nous serons en mesure de les comparer les uns aux autres et de faire ressortir les besoins d'un nouveau système, ainsi que les caractéristiques qu'il devrait améliorer.

2.1 Mise en situation

Depuis quelques années déjà, l'Internet prend de plus en plus d'importance dans la vie de tous les jours d'une partie croissante de la société. En utilisant les infrastructures actuelles de l'Internet, certains nouveaux instruments logiciels permettant d'effectuer numériquement des transactions changeront radicalement la façon d'interagir entre les commerces et leurs clients et induiront un accroissement encore plus rapide du commerce électronique à travers le monde [Hamilton, 1997].

Ayant satisfait les besoins de base pour assurer des communications faciles et rapides, le besoin d'effectuer des transactions numériques sur Internet devient de plus en plus évident. Toutefois, ce type de communication nécessite un niveau minimal de confiance, tant de la part des consommateurs que de la part des vendeurs. Ainsi, les acheteurs veulent s'assurer que la sécurité de leurs cartes de crédit, chèques ou portefeuilles virtuels n'est pas mise en danger et que les biens et services achetés en-ligne seront livrés. En même temps, les fournisseurs de biens et services veulent s'assurer qu'ils recevront les fonds correspondant aux marchandises vendues.

Le Web permet d'accéder rapidement et facilement à un nombre croissant de serveurs et de bases de données, partout dans le monde, ainsi que de travailler de façon ergonomique et transparente avec des applications multimédia, seulement en pointant et cliquant sur un écran, sans se préoccuper des protocoles de transmission, des types de données transmises, etc. Le Web s'adresse ainsi à tout le monde, sans nécessiter de préalables académiques.

Les instruments de navigation tels que Mosaic, Netscape Navigator ou Internet Explorer facilitent l'accès aux ressources électroniques sur toute la planète, en les apportant au bout des doigts ou d'un clic sur la souris. Ainsi, des usagers qui se

trouvent à des milliers de kilomètres seront capables d'effectuer des transactions commerciales, sous forme numérique, à l'aide de leurs ordinateurs personnels.

2.2 Problématique

La facilité avec laquelle les usagers de l'Internet peuvent créer du contenu informationnel, des pages Web qui peuvent être publiées en quelques secondes, a permis l'apparition rapide des magasins virtuels («*e-shops*», Fig. 2.1); si au début leur rôle principal était de tester la faisabilité du concept, peu après, leur but a changé afin de vraiment capitaliser sur la demande croissante pour faire des affaires numériquement. Des PME virtuelles aux grandes compagnies multinationales, chacun offre son propre site Web, souvent doté d'une zone réservée au commerce électronique.

Comme les informations disponibles aujourd'hui sur les réseaux publics de communication sont, dans une très vaste majorité, gratuites, les vendeurs potentiels de «propriété intellectuelle» ont peu de stimulants pour rendre disponibles leurs informations sur les réseaux; il y a pourtant un nombre croissant de vendeurs et de clients potentiels, prêts à vendre et à acheter ces informations. En même temps, d'autres modèles de vente et de marketing existent, comme nous allons voir dans le Chapitre 6, permettant aux marchands virtuels d'utiliser d'autres approches pour faire de l'argent, sans nécessairement facturer l'accès aux informations. Le seul aspect qui doit être implanté est un mécanisme sécurisé et ergonomique pour traiter les transferts de fonds à travers ces nouveaux médiums électroniques. Comme une grande majorité des transactions ne dépassent pas quelques dollars, la seule méthode efficace de les traiter doit être automatique. L'utilisation d'un tel système permettra un accroissement encore plus rapide et plus large du commerce électronique à travers le monde.

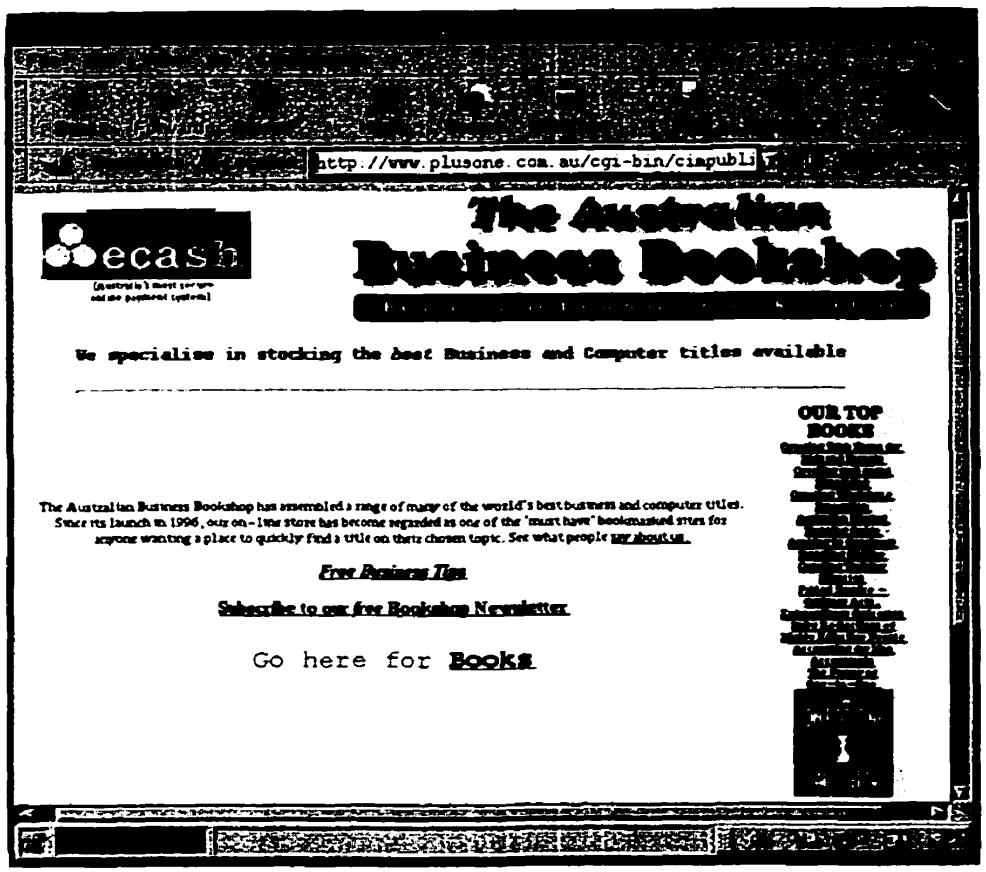

Figure 2.1 – *Un exemple de magasin virtuel sur le Web*

Le défi du commerce électronique est donc de permettre l'échange des produits et des services de façon efficace, rapide et sécuritaire, tout en maintenant les coûts de transaction à un niveau raisonnable et compétitif avec les modalités transactionnelles déjà existantes. Par ailleurs, face à la diversification sans précédent de l'offre d'informations juste-à-temps et des nouveaux besoins de l'économie du savoir, une autre tâche importante sera de permettre l'introduction de ce qu'on appelle le concept de ***micropaiements***, qui permettra d'effectuer des transactions sur des quantités infimes de valeur ou d'information, augmentant ainsi non seulement la granularité[1]

[1] Nous définissons le terme ***granularité*** comme étant le plus petit montant tangible d'une devise qui peut être utilisé comme incrément pour effectuer un paiement.

d'une devise, mais aussi le potentiel commercial des fournisseurs d'informations, produits ou services en général.

Nous pouvons donc conclure que l'achat (ou la vente, respectivement) de biens et services sur un réseau informatique implique deux sortes de transferts: le transfert des biens et services du vendeur au client, et, en contrepartie, le transfert électronique d'argent du client au vendeur. Si le transfert de biens ou services peut se faire moyennant des méthodes traditionnelles de transfert, incluant, par exemple, le courrier express, l'intérêt du système de transfert numérique de la valeur est d'effectuer une transaction utilisant comme seul support les réseaux informatiques.

La notion de commerce électronique regroupe plusieurs aspects, en partant des catalogues en-ligne et des paniers électroniques, jusqu'à l'Échange de Documents Informatisés (EDI) et la facturation électronique. Comme la structure de base d'un transfert de valeur quelconque suit fidèlement le modèle d'un paiement, nous allons nous concentrer sur ce dernier aspect, c'est-à-dire, sur les systèmes permettant d'effectuer des paiements sur Internet.

Il est important de noter que, dans le cadre de cet ouvrage, nous allons faire une distinction claire entre le commerce électronique et les outils de paiement électronique. Ainsi, le commerce électronique fait référence à un concept général, comprenant l'ensemble des actions transactionnelles réalisées à l'aide de l'informatique, des réseaux et des autres moyens numériques. Cette notion inclue des aspects divers, tels que les activités promotionnelles, les aspects fonctionnels – catalogues, listes ou paniers électroniques –, les méthodes de paiement, les aspects législatifs concernant la facturation, l'imposition et la taxation, etc. Par contre, le paiement électronique est seulement une opération parmi plusieurs actions constituant le commerce électronique. Ainsi, dans toute transaction, le paiement est un moment crucial qui complète l'acte d'acheter et de vendre. Concrètement, au niveau d'un système informatique, le paiement

est soit un parmi plusieurs modules constituant une solution complète de commerce électronique, soit un système indépendant fourni de façon autonome, qui est intégré à d'autres modules pour former un système complet de commerce électronique.

La notion de paiement est un élément intrinsèque de toute transaction commerciale; dans le monde virtuel, les systèmes de paiement électronique essaient soit d'émuler des méthodes et des mécanismes transactionnels du «monde réel», soit d'innover la façon par laquelle les transactions s'effectuent. Même si la plupart des solutions de paiement interentreprises («*business-to-business*») sont encore basées sur EDI – cependant cette solution perd rapidement du terrain en faveur de solutions alternatives –, la plupart des systèmes de paiement sur Internet s'adressent exclusivement aux consommateurs. Aux deux niveaux, le besoin pour des standards, pour de la compatibilité et de l'interoperabilité, pour des outils faciles à utiliser, ont conduit à une convergence de plus en plus évidente autour de l'Internet.

Aujourd'hui, dans cette nouvelle ère informationnelle, la manipulation électronique des documents numériques est devenue ubiquiste. Le support électronique s'est avéré d'une très grande valeur pour toutes les informations qu'il peut contenir, des livres numérisés aux documents en format hypertexte. Tout le monde a découvert les gains de productivité et les réductions des coûts engendrés par ce nouveau moyen de créer, de diffuser, d'échanger ou de stocker les connaissances.

La quantité énorme de documents numériques déjà disponibles rend évident le potentiel commercial de ce nouveau médium. Dans une ère où presque tout peut être numérisé et rendu dans un format électronique, l'achat et la vente de bits d'information deviendra la colonne vertébrale d'une nouvelle économie. Ainsi, de nouvelles opportunités financières apparaissent; qu'elles soient représentées par des réductions de coûts, de gains de productivité ou par des nouveaux moyens pour faire des affaires en-ligne, le potentiel pour des profits rapides n'est nullement négligeable.

2.3 Définitions et généralités

Afin de bien pouvoir comprendre les tendances et les différences entre les diverses méthodes d'échange de valeurs dans différents environnements économiques, nous introduisons ici quelques notions générales. Parmi les nombreux systèmes transactionnels existants aujourd'hui, traditionnels ou électroniques, plusieurs notions générales ressortent de façon constante, notions servant à bien identifier, départager et comprendre les différentes tâches et fonctions d'un système de paiement.

2.3.1 Les entités transactionnelles

Dans cet ouvrage, nous allons utiliser le terme ***document*** (électronique ou non) pour représenter tout objet ayant une valeur quelconque, tels que des pièces, coupons ou billets (numériques ou non), ainsi que d'autres informations (textes, cartes, dessins, etc.). Un ***document électronique*** représentera donc un tel objet dans le monde virtuel, et prendra la forme d'un fichier binaire qui n'a pas de valeur intrinsèque mais qui pourrait être transigé numériquement. Ces documents peuvent subir différentes manipulations dans le système transactionnel. Un ensemble de manipulations peut, lorsqu'elles sont arrangées dans un ordre bien défini, former un ***protocole transactionnel***.

Un système transactionnel échange, sous une forme ou une autre, de l'argent, réel ou virtuel, ou d'autres types de documents ayant une valeur non-intrinsèque quelconque. Ces documents sont manipulés de différentes façons par les acteurs du système, où chaque ensemble d'acteurs ayant les mêmes propriétés et fonctions forme une ***entité***.

Généralement, un système de transfert de valeurs comprend quatre entités – le client, le vendeur, l'émetteur et la banque. Nous résumons dans la liste qui suit les principales caractéristiques spécifiques à chacune des entités:

1. **Le client**

- ouvre (et ferme) des comptes à la banque;
- dépose (et retire) des pièces, billets ou autres documents à la banque;
- dépense (et reçoit – dans les systèmes symétriques, que nous allons définir dans les sections suivantes) des pièces, billets ou autres documents auprès d'un vendeur – ou auprès d'autres clients – contre des produits, services ou autres documents.

2. **Le vendeur**

- est lui-même un client et peut donc effectuer toutes les opérations que les clients ordinaires effectuent;
- peut effectuer (dans les systèmes hors-ligne, que nous allons définir dans les sections suivantes) la vérification locale et indépendante des paiements reçus;
- de plus, possède généralement une capacité de stockage supérieure, et un serveur de requêtes – par exemple un serveur Web.

3. **L'émetteur**

- émet et libère des pièces, billets ou autres documents;
- signe et certifie les pièces, billets ou documents émis;
- négocie et transmet à la banque les pièces, billets ou autres documents émis, en échange d'une contre-valeur équivalente accompagnée d'une rémunération quelconque, établie de commun accord.

4. **La banque**

- ouvre (et ferme) les comptes des clients;
- accepte (ou rejette) les dépôts et les retraits;
- accepte (ou rejette) les pièces, billets ou autres documents en transit;
- authentifie les pièces, billets ou autres documents utilisés et renouvelle les pièces ou les billets expirés;
- valide les transactions;
- négocie et reçoit de l'émetteur les pièces, billets ou autres documents émis, en échange d'une contre-valeur équivalente accompagnée d'une rémunération quelconque, établie de commun accord.

Notons que la plupart du temps, l'émetteur et la banque peuvent former une seule et même entité. Les quatre entités du système interagissent les unes avec les autres suivant un protocole (qu'il soit sur une plate-forme électronique ou non). Nous allons utiliser le terme ***en-ligne*** pour désigner les transactions où une connexion TCP/IP directe est réalisée entre le client (ou le vendeur, tout dépendant du système) et la banque. Dans le même contexte, une transaction qui n'est pas en-ligne sera appelée ***hors-ligne***; dans ce cas, la transaction est soit différée, soit réalisée par d'autres moyens de communication (par courrier électronique, à l'aide d'une disquette, etc.). Ainsi, nous définissons le ***vendeur*** – appelé aussi le marchand – comme étant la source d'un transfert (ou d'un transport ou échange) de documents, que ce soit ou non un paiement. L'***acheteur*** acquiert ces documents, en étant la destination du transfert. L'***émetteur*** est l'entité qui crée, signe et certifie les documents qui circulent dans le système. Enfin, l'entité ***banque*** vérifie, conserve temporairement ou archive dans ses bases de données les documents transigés par ses clients – les acheteurs et les vendeurs. Pour des applications financières, les banques acquièrent des licences et des pièces et billets auprès d'un ou plusieurs émetteurs; pour des applications non-financières, elles comparent, vérifient, échangent, conservent ou archivent des documents pour leurs clients.

2.3.2 Les modalités traditionnelles de paiement

Au cours des dernières années, la croissance rapide de l'Internet a rendu de plus en plus évidente la nécessité de l'utilisation des moyens numériques pour effectuer des échanges commerciaux dans le monde virtuel. Le concept de commerce électronique a été déjà identifié comme étant une technologie ayant un très haut potentiel, pouvant générer de nouvelles sources de revenus, de meilleurs gains de productivité et ainsi de meilleurs retours sur l'investissement.

Les commerces n'ont donc pas attendu l'apparition et l'introduction d'un standard international pour les paiements électroniques [Anderson, 1997]. À ce jour, plusieurs compagnies vendent déjà leurs produits et services sur l'Internet à l'aide des méthodes traditionnelles de paiement [Asokan et al., 1997]: les chèques ou mandats et les cartes de crédit.

2.3.2.1 L'argent comptant

En effet, parmi les méthodes de paiement – et plus généralement de transfert de valeur – qui sont disponibles de nos jours, certaines ne peuvent pas être utilisées sur les réseaux électroniques. Ainsi, l'argent comptant est le premier à être éliminé, son transfert électronique à distance étant impossible. Même pour le transfert physique, les consommateurs utilisent d'autres moyens de transport, tels que les mandats postaux.

2.3.2.2 Les chèques ou mandats

Les premiers paiements pour des produits et services sur Internet ont été effectués (et sont toujours effectués, dans une grande mesure) à l'aide des chèques ou mandats envoyés par la poste au vendeur. Cette méthode n'est pas seulement encombrante et incommode, mais elle prend plusieurs jours et elle est aussi très

coûteuse, car chaque mandat ou chèque peut coûter 0.50$, 1.00$, 2.00$ ou plus. Cette méthode n'est donc pas utilisable pour payer des services à faible coût, tels que les recherches d'informations ou de nouvelles, les cotations boursières, etc. Cela revient à payer quelques cents pour le service, 50 cents pour le chèque et 50 cents pour le timbre !

2.3.2.3 Les cartes de crédit

Pour prévenir ces coûts et ces inconvénients, les cartes de crédit offrent des possibilités moins dispendieuses. Pour payer un service, il suffit de simplement envoyer – par exemple, par courrier électronique – le numéro de la carte chez le vendeur, qui va débiter le compte. Toutefois, cette méthode implique de grands risques, étant donné qu'il faut envoyer des informations confidentielles sur des réseaux non-sécuritaires. Si le message est intercepté en cours de route par un malfaiteur, il pourra utiliser ces informations de façon illicite, causant d'importantes pertes aux utilisateurs.

2.3.3 Les nouvelles modalités de paiement

Le paiement électronique sur Internet pose plusieurs problèmes différents, tels que: les modalités techniques de paiement, la protection des intérêts des entités transactionnelles, la confidentialité des données transmises [Phillips, 1997], l'authentification des entités [Opplinger, 1996], [Opplinger, 1997] ou la sécurité du transfert d'information [Atkinson, 1997]. La plupart des faiblesses rencontrées dans les systèmes de paiement traditionnels, qui ne répondent pas aux exigences de l'Internet, ont été corrigées depuis quelques années. Ainsi, face aux nouveaux besoins des consommateurs, plusieurs méthodes modernes de paiement ont été introduites ou proposées. Nous allons regarder dans les pages qui suivent les concepts généraux sur lesquels ces méthodes sont basées.

2.3.3.1 Les transferts bancaires

Cette nouvelle méthode de paiement, utilisant les cartes bancaires de débit, a été introduite il y a quelques années sur le marché, avec un grand succès. Elle consiste à transférer automatiquement et directement, du compte du client dans celui du vendeur, le montant de la transaction. Cette méthode implique l'utilisation d'un équipement spécial capable de lire la carte de débit ainsi que le NIP (Numéro d'Identification Personnel) du client, et de les communiquer à la banque. Inversement, un employeur peut verser le salaire d'un employé, à l'aide d'un dépôt direct, dans un compte préétabli. Ce type de transaction n'est disponible toutefois qu'aux institutions.

En ce qui concerne le paiement direct, par carte de débit, l'équipement matériel implique un investissement supplémentaire et n'est habituellement disponible que du côté du vendeur. Par ailleurs, le système n'est pas disponible sur les réseaux de communications non-bancaires et donc, reste inutilisable sur Internet.

2.3.3.2 Les cartes intelligentes

Les «cartes intelligentes» ou «*smart-cards*» sont des cartes en plastique contenant un microcontrôleur ou un microprocesseur. Généralement, elles emploient un système de débit, c'est-à-dire, elles doivent être payées d'avance. La valeur emmagasinée peut être dépensée auprès de vendeurs équipés de lecteurs capables de lire ces cartes [Gallant, 1995]. Au Québec, plusieurs de ces systèmes fonctionnent déjà, par exemple, la carte téléphonique «La Puce» de **Bell**.

Les cartes intelligentes contiennent généralement un compteur pour stocker les fonds et un témoin [Brands, 1994b] pour éviter toute tentative de fraude; la méthode apporte une grande commodité et fiabilité, est plus difficilement falsifiable et moins complexe, mais requiert des modules matériels assez coûteux. Par contre, une solution

exclusivement logicielle est beaucoup moins dispendieuse mais, dans son ensemble, elle est sensiblement plus complexe que celle basée sur les cartes intelligentes.

Le grand avantage de tout système utilisant des cartes intelligentes réside dans sa capacité de permettre des transactions «sur la rue», sans utiliser d'ordinateurs. Aussi, en fonction de la capacité physique du microprocesseur incorporé dans la carte, d'autres informations utiles, et même des valeurs, peuvent être emmagasinées; la future Carte Soleil (carte d'assurance maladie), au Québec, constitue un bon exemple de cette approche. Ce système utilise toutefois des lecteurs de cartes dédiés ainsi que des réseaux privés de communication ce qui implique d'importants investissements initiaux et restreint la capacité de participation des utilisateurs potentiels.

Des applications de fidélisation des clients sont aussi possibles. Dans cette catégorie nous pouvons retrouver, entre autres, les points boni pour les acheteurs ou les voyageurs réguliers, les coupons électroniques, les cartes cadeaux prépayées ou les cartes d'accès aux chambres d'hôtel. Des détaillants comme **Wal-Mart** ou **Burger King** sont en train d'évaluer plusieurs projets pilote qui utilisent soit des cartes intelligentes soit des cartes magnétiques. De tels systèmes de fidélisation sont très utiles et importants pour trois raisons principales: ils augmentent les dépenses par client, ils lient les clients aux marques commerciales et ils augmentent les parts de marché des vendeurs qui les utilisent.

2.3.3.3 L'encryptage des numéros de cartes de crédit (les chèques électroniques)

Une solution intéressante a été apportée par plusieurs compagnies, parmi lesquelles **Netscape Communications**. Elle consiste à inclure dans les interfaces du Web des mécanismes cryptographiques capables d'encoder les informations confidentielles, telles que les numéros de cartes de crédit, et donc de sécuriser cette

méthode de paiement. SSL (*Secure Sockets Layer*) [Référence électronique SSLP] est l'un de ces protocoles; il connaît un grand succès et il est devenu le standard *de-facto* pour la transmission des numéros de cartes de crédit à l'aide d'un fureteur. De la même façon, le numéro de compte de chèques du client peut être envoyé aux vendeurs acceptant ce type de paiement.

Même si cette méthode est en elle-même une solution tout à fait viable, elle conserve quelques inconvénients, tels que le coût des transactions, qui rend impraticables les minipaiements – transactions à faible coût, de 1 à 10 $ – ainsi que les micropaiements, tels que les paiements à l'utilisation (par exemple, lorsque chaque transaction est facturée de 15 cents par la compagnie de crédit, alors que l'information achetée ne coûterait que 2 cents). De plus, en utilisant une carte de crédit, les compagnies de crédit et les banques peuvent accumuler des statistiques sur les habitudes d'achat des consommateurs, établissant ainsi le profil de chaque client afin de lui envoyer différents types de publicité personnalisée, portant ainsi atteinte à sa vie privée. Le système est «asymétrique», dans le sens où, l'équipement (matériel/logiciel) du vendeur n'est pas le même que celui du client.

2.3.3.4 Les chèques électroniques certifiés

Cette méthode de paiement – dite «indirecte» – peut être définie comme utilisant un tiers pour effectuer une transaction. Une compagnie (telle que **NetBank** [Netbank, 1995]) collecte l'argent des clients, sous forme de chèques ou mandats, et libère en échange des chèques numériques certifiés, en clair ou sous forme de messages encryptés, envoyés par courrier électronique, en approuvant chaque transaction séparément. Si la méthode est effectivement viable, elle présente un défaut assez important: une transaction n'est pas réalisée en direct, en-ligne, mais plutôt par courrier électronique, ce qui non seulement prend beaucoup plus de temps (de quelques minutes à quelques jours) mais fait aussi perdre le caractère ergonomique des transactions.

2.3.3.5 Les coupons électroniques

Les «coupons électroniques» [Flohr, 1996] sont les équivalents numériques des coupons de supermarchés. Leur mode d'emploi est semblable à celui des chèques électroniques (avec les avantages et les désavantages afférents), avec deux exceptions notables: ils peuvent être utilisés seulement auprès de l'institution émettrice, et ils représentent généralement des produits ou services – sans permettre un échange contre de l'argent comptant.

2.3.3.6 L'argent électronique

Le **Ministère des Finances des États-Unis** (*The U.S. Department of Treasury*) a publié récemment la définition suivante: «*L'argent électronique est une note ou un titre émis par un émetteur, stockée sous forme de code informatique sur une carte de la taille d'une carte de crédit ou sur le disque dur d'un ordinateur. Les consommateurs achètent cette note avec de l'argent traditionnel. Ils l'échangent contre des biens et des services auprès de marchands qui acceptent de considérer cette note comme un paiement*». Ce type de système transactionnel est conçu pour tirer profit des avantages des deux méthodes précédentes, tout en minimisant ou éliminant leurs désavantages et inconvénients. De façon générale, la méthode consiste à transmettre des «pièces», «notes» ou «billets» numériques qui ont une valeur monétaire, étant payés d'avance.

Ce dernier type de système transactionnel offre non seulement la sécurité nécessaire pour le transfert de valeurs, par l'intermédiaire des méthodes puissantes d'encryptage, mais il offre aussi la commodité des transactions en-ligne de type «pointer et cliquer», sans avoir à sortir de l'interface graphique, ou bien, en utilisant une carte intelligente, format carte de crédit [Fancher, 1997]. Il offre aussi, dans certains cas, l'anonymat des transactions [Chaum, 1981], [Bürk et Pfitzmann, 1989], [Chaum, 1989],

[Chaum, 1992], [Low et al., 1994] en s'assurant que personne ne peut retracer une transaction et faire ainsi un lien entre un client et ses achats.

Plusieurs applications peuvent utiliser avec succès ce nouveau concept. En plus des transactions rapides et ergonomiques – pointer et cliquer –, le système peut être utilisé pour effectuer des paiements périodiques automatisés, par exemple le paiement automatique des factures. À l'aide d'un équipement spécial (émetteur/récepteur infrarouge ou carte à puce), le système peut également être utilisé pour effectuer le paiement du stationnement, du transport en commun ou des péages sur l'autoroute sans que les véhicules s'arrêtent.

Une autre application extrêmement intéressante est celle des micropaiements [Manasse et al., 1995]. Le système permet de raffiner la granularité d'une devise (par exemple: au Canada, 1 cent; en France, 5 centimes, etc.) pour permettre des paiements à l'utilisation pour des services à faible valeur, tels que les services fréquents – comme les recherches de titres de nouvelles – qui valent moins d'un cent, ou des montants fractionnaires, comme 1.5 cents, etc. Cette nouvelle forme de représentation monétaire reproduit fidèlement l'argent comptant. Physiquement, l'argent virtuel est constitué par des fichiers binaires contenant plusieurs champs, parmi lesquels on retrouve une valeur nominale, un numéro de série et une ou plusieurs signatures numériques. Comme dans le «monde réel», ce type de représentation monétaire a la particularité d'appartenir «au porteur» et très souvent des moyens pour assurer l'anonymat sont inclus dans les protocoles transactionnels; il est donc impossible de retracer ces transferts des fonds.

Un problème majeur qui doit être évité dans tous les systèmes transactionnels est l'accès non-autorisé aux données et au fonds privés des utilisateurs. Les moyens cryptographiques et de contrôle d'accès – comme les mots de passe – protègent assez bien contre ce type de fraude. Par contre, le problème des «dépenses

multiples», propre aux systèmes basés sur l'argent virtuel, est plus compliqué. En effet, comment peut-on s'assurer qu'un billet virtuel n'a pas été copié plusieurs fois et dépensé auprès de différents vendeurs de façon illicite ? Différents moyens de vérification, utilisant principalement le numéro de série du billet, protègent le système contre ce type de fraude, tandis que des moyens pour retrouver le faussaire, en retraçant ses coordonnées, sont toujours inclus dans les protocoles de paiement employant l'argent virtuel.

2.4 Systèmes de paiement sur Internet

2.4.1 Description d'une transaction numérique typique

Plusieurs types de protocoles sont offerts aujourd'hui aux consommateurs désireux de transiger sur Internet, utilisant différentes façons de représenter les fonds échangés; que ce soit des cartes de crédit, des chèques ou de l'argent virtuel, la ***représentation monétaire*** (RM) employée est cruciale pour déterminer précisément le protocole suivant lequel le transfert de fonds prendra place. Si la plupart des systèmes de paiement numérique sur Internet s'inspirent du «monde réel», plusieurs systèmes innovent en introduisant de nouvelles façons de transiger dans le monde virtuel.

En se basant sur les définitions effectuées dans les sous-sections précédentes, regardons comment s'effectue généralement une transaction, qui sont les acteurs impliqués et quels sont leurs rôles: tout d'abord il y a un acheteur, qui désire échanger son argent contre des biens ou services offerts en-ligne par un vendeur, à l'aide d'un intermédiaire, ou courtier virtuel, qui effectue le traitement des transactions; cet intermédiaire peut être soit un autre vendeur soit une banque. Cette banque gère les

comptes des clients et des vendeurs et effectue l'acquittement et le clearing des transactions. Enfin l'émetteur – généralement une banque – émet la représentation monétaire utilisée dans le système et protège la qualité de cette représentation monétaire, et ainsi, les valeurs qu'elle représente.

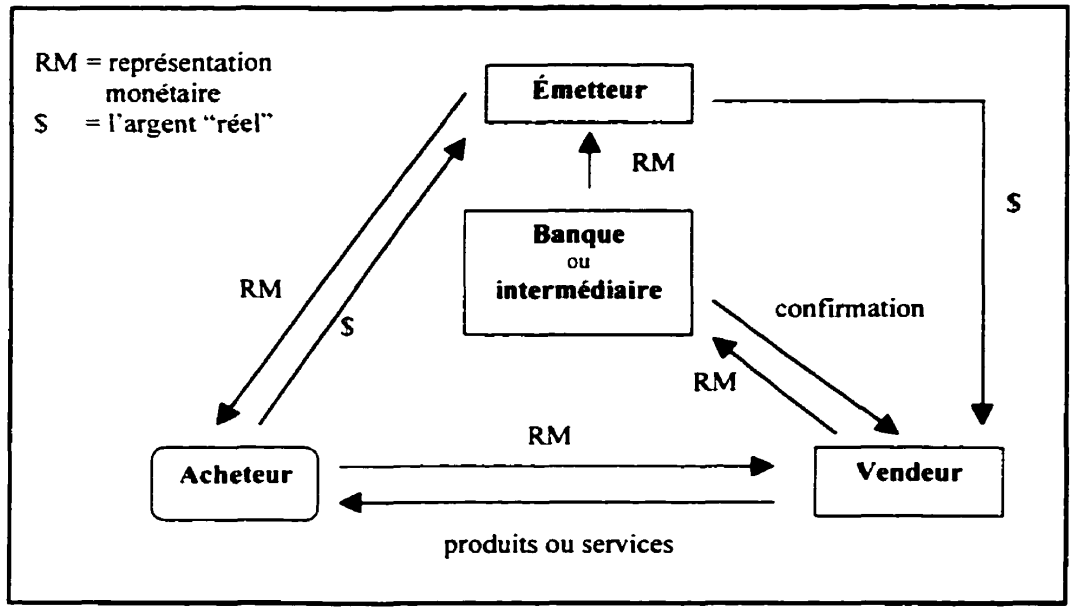

Figure 2.2 – *Le flux transactionnel d'un système numérique de paiement*

Comment s'effectue la transaction numérique ? Sans faire référence à un protocole en particulier, la Figure 2.2 décrit un flux transactionnel générique. De façon générale, un client transmet la RM – qui dépend du système utilisé – au vendeur, qui peut la vérifier en l'envoyant à l'intermédiaire ou directement à la banque. Suivant cette vérification, le vendeur reçoit – le cas échéant – une confirmation et peut livrer la marchandise au client. L'acheteur achète – au préalable (dans certains systèmes) ou ultérieurement (dans d'autres) – cette représentation monétaire auprès de l'émetteur; ce dernier peut aussi rembourser le vendeur sur demande, suivant certaines règles préétablies.

2.4.2 Taxonomie

Nous introduisons dans cette sous-section une série de critères de classification qui nous permettront de faire ressortir les avantages et les inconvénients de chacun des systèmes étudiés dans le cadre de la recherche bibliographique quasi exhaustive que nous avons effectuée. Ainsi, nous serons capables de trouver quels sont les besoins qu'un éventuel nouveau système devra combler et comment ce système pourra se comparer aux autres systèmes existants.

La recherche bibliographique que nous avons effectuée comprend non seulement une recherche en profondeur des documents imprimés – livres ou revues recherchées sur CD-ROM –, mais surtout un vaste effort de résumer les publications électroniques, aussi bien au niveau des sites Web, qu'au niveau des articles dans les groupes électroniques de discussions sur le sujet et des groupes de nouvelles, partagés par les chercheurs de ce domaine. Cette recherche nous a permis aussi de construire une vaste liste de ressources électroniques, incluse dans une section distincte de la bibliographie. Notons que dans le cadre de nos recherches, nous nous sommes concentrés exclusivement sur le contexte des réseaux publics, en l'occurrence l'Internet. Nous allons donc traiter uniquement des modes de paiement et des systèmes de sécurisation des transactions disponibles ou utilisables sur Internet – que ces systèmes soient autonomes ou qu'ils fassent partie d'une solution de commerce électronique complète, qui comporte souvent plusieurs autres modules: catalogues, paniers d'épicerie, modules de facturation et même des modules de paiement et d'EDI. Étant donné le nombre croissant de systèmes numériques de paiement, les méthodes permettant de les classifier, de les analyser et de les évaluer deviennent très utiles pour tous ceux qui désirent déployer et utiliser dans un futur rapproché de tels systèmes transactionnels. Pour ce faire, nous introduisons une taxonomie permettant de classifier les systèmes de paiement numérique sur Internet selon différents facteurs [Ureche et Plamondon, 1998b].

Afin de pouvoir diviser la multitude de systèmes existants en plusieurs catégories, nous introduisons quelques critères de classification. Ces critères sont très flexibles, conçus de manière à permettre, sans changements majeurs, l'inclusion dans notre classification des systèmes qui apparaîtront sûrement dans les années à venir. Ainsi, nous avons identifié deux aspects principaux qui peuvent fonder le squelette de notre classification: les exigences d'adhésion au système et la sécurité qu'un système offre. Le premier aspect fait référence aux exigences d'un système de paiement sur Internet concernant l'inscription et l'abonnement au système, et possiblement la nécessité de télécharger les outils nécessaires pour l'utiliser. Le deuxième aspect regarde tous les éléments de protection du système, ainsi que le modèle de sécurité employé.

Les modèles nécessitant une adhésion (ou un abonnement) ont intrinsèquement un niveau minimal de sécurité, représenté par au moins un numéro d'abonnement, un mot de passe ou un *cookie*[2]. Les systèmes sans adhésion emploient le modèle de «transaction unique» et sont généralement utilisés par des fureteurs comme Netscape Navigator ou Internet Explorer et sont basés sur le protocole SSL. Plusieurs vendeurs, afin d'attirer des clients qui n'ont pas de fureteurs ayant des fonctions cryptographiques de sécurité, offrent encore des méthodes de paiement non-protégées.

À partir de ce premier aspect fondamental, les systèmes peuvent être divisés en deux grandes ***catégories*** suivant la nécessité d'effectuer ou non une adhésion au système. Une catégorie représente donc une définition générale, de haut niveau, d'un ensemble de systèmes ayant les mêmes exigences d'adhésion. Cette structure de base est raffinée ensuite à l'aide de l'autre aspect principal, l'aspect sécurité.

---

[2] Fichier envoyé par le serveur Web d'un vendeur, contenant des informations telles qu'un numéro de série (constituant en quelque sorte un mot de passe), une date d'émission et, possiblement, une date d'expiration.

Ainsi, chacune des deux catégories contient plusieurs ***classes***, en fonction du modèle transactionnel employé et du niveau de protection offert – par exemple, le modèle «sans protection», le modèle «débit-crédit», le modèle «comptant», etc. Dans la plupart des cas, ces modèles sont basés sur des modèles transactionnels existants, tels que ceux utilisant des instruments bancaires de paiement, ceux utilisant l'argent liquide, etc. De cette façon, une classe est la représentation virtuelle d'un modèle de sécurité ou d'un modèle transactionnel du «monde réel».

Tableau 2.1 – *Taxonomie*

Catégorie	Classe	Groupe
I – SYSTÈMES SANS ADHÉSION		
	1) Modèle «sans protection»	
		a) cartes de crédit / chèques
	2) Modèle «avec protection» (en général encryptage avec SSL)	
		a) cartes de crédit
		b) chèques
II – SYSTÈMES AVEC ADHÉSION		
	1) Modèle «authentification»	
		a) mots de passe / *cookies*
		b) «dépôt légal»
	2) Modèle «débit-crédit»	
		a) NIP / mots de passe
		b) chèques électroniques
		c) facturation / cartes de crédit
	3) Modèle «comptant»	
		a) pièces numériques / billets virtuels

À son tour, chaque classe contient un ou plusieurs ***groupes*** de systèmes de paiement reflétant la technologie de transfert de fonds employée – par exemple, les

systèmes basés sur les mots de passe, les chèques électroniques, la facturation et les cartes de crédit, l'argent virtuel, etc. Ainsi, un groupe constitue un ensemble de systèmes qui utilisent une même technologie de transfert de fonds.

De temps en temps, un ***sous-groupe*** peut être formé lorsque plusieurs systèmes ayant certaines similarités basées sur la technologie de transfert sous-jacente à leur groupe ont été proposés ou implantés. Ainsi, les systèmes basés sur le standard SET (*Secure Electronic Transaction*) forment un sous-groupe du groupe «facturation / cartes de crédit», puisqu'ils utilisent tous – le groupe et le sous-groupe – les mêmes moyens pour transférer des fonds. De la même façon, les systèmes permettant d'effectuer des micropaiements forment un sous-groupe du groupe «pièces et billets virtuels». Nous résumons cette nouvelle taxonomie dans le Tableau 2.1.

2.4.3 Critères d'analyse et d'évaluation

À l'aide du Tableau 2.1, nous sommes capables d'effectuer une classification claire et complète des systèmes de paiement existants sur Internet. Après les avoir classifiés, nous pourrons les analyser et les évaluer afin de les comparer les uns aux autres et de faire ainsi ressortir leurs avantages et leurs inconvénients respectifs. Pour ce faire, nous allons tout d'abord introduire une série de critères d'analyse et d'évaluation.

Pour faciliter la compréhension, nous avons divisé en deux parties la liste des critères d'analyse et d'évaluation des systèmes électroniques de paiement sur Internet. Ainsi, tous les éléments qui sont intrinsèquement reliés au fonctionnement interne d'un système sont regroupés dans un premier ensemble, appelé «les caractéristiques internes du système». De la même manière, tous les éléments qui aident les différentes entités d'un système de paiement sur Internet à amorcer, effectuer ou

terminer leurs tâches, de même que tous les éléments qui complètent ce système, sont regroupés dans un deuxième ensemble appelé «les caractéristiques externes du système». Le Tableau 2.2 résume la liste des critères, ainsi que les valeurs que chacun peut prendre.

Tableau 2.2 – *Critères d'analyse et d'évaluation*

Critère	Valeurs possibles
1er ensemble: les caractéristiques internes	
a) Sécurité	faible, moyenne, forte, très forte
b) Représentation monétaire (RM)	mots de passe & NIP, compteurs & numéros de série, certificats numériques, pièces numériques & billets virtuels
c) Pérennité de la RM	usage unique, limitée, illimitée
d) Configuration du système	asymétrique, symétrique
e) Niveau d'anonymat	bas, moyen, haut
f) Granularité de la RM	grossière, moyenne, raffinée, arbitrairement raffinée (ajustable)
2ème ensemble: les caractéristiques externes	
a) Débit de fonds	anticipé, différé
b) Délai d'encaissement	long, moyen, court
c) Mode d'échange des fonds	en-ligne ou indirect, hors-ligne ou direct
d) Convertibilité de la RM	nulle, limitée, totale
e) Niveau de développement	recherche, expérimentale, exploitation commerciale

Regardons de plus près chacun de ces critères, ce qu'ils signifient, ce qu'ils représentent, ainsi que les valeurs qu'ils peuvent prendre.

2.4.3.1 Les caractéristiques internes d'un système

a) Sécurité

Une première caractéristique, de très grande importance, est le niveau de sécurité assuré par un système de paiement. En effet, cette caractéristique intrinsèque a toujours un impact majeur sur le niveau de confiance que les utilisateurs ont dans le système, tant au niveau des clients et des vendeurs, qu'au niveau des banques et des

émetteurs. Ainsi, les clients veulent protéger leurs fonds contre toute perte ou tentative de vol. Les vendeurs veulent recevoir les paiements correspondants aux biens ou services vendus et vont essayer de protéger leurs marchandises contre toute tentative de fraude. Les banques veulent protéger les comptes des clients ainsi que la qualité de leurs services d'intermédiaires. Enfin, les émetteurs veulent protéger la qualité de la représentation monétaire émise qui circule dans le système, et ainsi, les valeurs qu'elle représente.

Nous employons cinq sous-critères afin de mieux expliciter le critère de sécurité. La ***disponibilité***, ou le contrôle d'accès, réfère à l'accès au système ou aux données qui circulent à l'intérieur de ce système; par exemple, ceci peut être réalisé à l'aide de l'encryptage: seuls les usagers détenant des clés valides peuvent participer aux échanges. L'***authentification*** fait référence à la capacité d'un système de démontrer à toute entité intéressée la vraie source d'un message transactionnel. L'***intégrité*** est un sous-critère qui réfère à la protection du contenu de chaque message transactionnel, afin d'empêcher tout changement en cours de route, avant d'atteindre le destinataire. La ***confidentialité*** assurée par un système porte sur sa capacité de garder secrètes les informations transmises et de ne révéler aux entités concernées que les informations qui sont strictement nécessaires au bon fonctionnement des transactions. Enfin, la ***non-répudiation*** est la capacité d'un système de paiement de ne pas permettre la révocation arbitraire d'une transaction, protégeant ainsi toutes les entités concernées.

Pour mieux résumer la sécurité d'un système de paiement sur Internet, nous introduisons des qualificatifs globaux. Ainsi tout système qui ne rencontre aucun ou qu'un seul sous-critère parmi les cinq mentionnés, offre une sécurité faible. Un système remplissant deux ou trois des cinq sous-critères offre une sécurité moyenne, tandis qu'un système qui remplit tous les sous-critères sauf un, offre une sécurité forte. Enfin, lorsque tous les sous-critères sont rencontrés, la sécurité du système est considérée comme étant très forte. Notons que ces qualificatifs globaux ne sont pas absolus, ils sont

plutôt relatifs et servent d'indicatifs; nous n'avons pas utilisé dans cette approche le qualificatif de sécurité «totale», étant donnée la possibilité grandissante des techniques de cryptanalyse de calculer et révéler rapidement les clés de certains algorithmes cryptographiques et ce, malgré la constante évolution des moyens de sécurisation.

b) Représentation monétaire

La représentation monétaire est constituée par l'information transmise entre les différentes entités transactionnelles et est déterminée par le type de système de paiement. Elle va déterminer ainsi le support matériel et logiciel qui lui est nécessaire pour effectuer le transfert de fonds, ainsi que l'acquittement et le clearing interbancaire.

Cette information peut prendre la forme d'un NIP numérique ou d'un mot de passe alphanumérique. Elle peut aussi prendre la forme de compteurs (surtout dans les cartes intelligentes) ou de numéros de série, encryptés ou non – qui peuvent contenir un numéro de compte, de carte de crédit, de transaction, etc. Elle peut aussi prendre la forme de certificats numériques – documents électroniques qui contiennent, entre autres, un numéro de série, une date d'émission, une date d'expiration, le nom de l'émetteur ainsi que sa signature numérique [Ford, 1998].

Enfin, la RM peut être constituée par des pièces numériques ou des billets virtuels – fichiers binaires contenant, entre autres, une valeur nominale, un numéro de série ainsi qu'une ou plusieurs signatures numériques. Ces billets sont prépayés et ont ainsi une valeur monétaire dès leur émission. L'avantage évident de la méthode est qu'elle emploie véritablement de l'argent numérique, dans le sens où l'information transmise est effectivement une valeur. Le désavantage est un risque de contrefaçon plus élevé, risque qui ne peut être diminué que par un accroissement important de la complexité du système.

c) Pérennité de la RM

Un autre critère interne d'analyse et d'évaluation est constitué par la pérennité de la représentation monétaire transmise sur le réseau entre les différentes entités transactionnelles du système de paiement. Cette caractéristique interne concerne la capacité du système de réutiliser la représentation monétaire pour une ou plusieurs transactions subséquentes. Ainsi, d'un côté, certains systèmes permettent une longue durée de vie, voire une pérennité illimitée à leurs représentations monétaires, qui pourront alors être réutilisées sans restriction. D'un autre côté, il y a les systèmes qui emploient des unités à utilisation unique [Ferguson, 1993], qui nécessitent une nouvelle étape de génération de RM pour chaque transaction. En ce qui concerne les cartes intelligentes, la même classification peut être appliquée, étant donné le fait que certaines de ces cartes ne sont pas réutilisables (elles utilisent et brûlent des mémoires ROM) tandis que d'autres peuvent être rechargées.

d) Configuration du système

Un système est dit ***symétrique*** si l'ensemble de l'équipement matériel et logiciel du vendeur est tout à fait le même que celui du client, leur permettant ainsi d'échanger les rôles de façon arbitraire. Si, par contre, le vendeur doit s'équiper avec des modules spéciaux, soit matériels soit logiciels, auxquels le client n'a pas accès, le système est dit ***asymétrique***.

e) Niveau d'anonymat

De nos jours, la protection de la vie privée est un sujet qui intéresse de plus en plus les consommateurs. L'anonymat est une caractéristique intrinsèque d'un système de paiement qui permet de répondre à ce besoin. Ainsi, l'anonymat permet de garantir l'impossibilité de retracer une transaction: plus un système garantit un haut

niveau d'anonymat, moins il est facile de retrouver les traces d'un transfert de fonds, ce qui assure un grand niveau de confidentialité et de protection de la vie privée des consommateurs, mais, en même temps, ouvre la porte aux transactions illicites. En effet, l'anonymat donne la possibilité, entre autres, d'effectuer du blanchiment d'argent ou de l'évasion fiscale de façon facile, commode et rapide, sans laisser de traces, ce qui est socialement inacceptable.

f) Granularité de la RM

La granularité offerte par un système de paiement est déterminée par le plus petit montant qui peut être utilisé comme incrément pour effectuer un paiement. Dans le cas de l'argent réel, par exemple, au Canada ce montant est d'un cent, en France il est de 5 centimes, alors qu'en Italie il est de 10 lires.

Une granularité raffinée signifie un incrément minimal très petit, permettant l'utilisation de micropaiements pour effectuer de ***microtransactions***; par contre, les systèmes permettant d'effectuer des petits paiements mais qui ne raffinent pas la granularité de la devise utilisée, permettent d'effectuer des ***minipaiements*** seulement. Enfin, une granularité arbitraire, ou ajustable, signifie une totale flexibilité quant aux incréments minimes à utiliser dans une transaction.

2.4.3.2 Les caractéristiques externes d'un système

a) Débit de fonds

Nous utilisons ce critère d'analyse et d'évaluation pour déterminer si le transfert effectif des fonds a lieu avant ou après la transaction. La plupart des systèmes basés sur des coupons ou billets numériques requièrent un paiement ***anticipé***, donnant ainsi à ces unités de transfert électronique une valeur monétaire dès leur émission. Par

contre, les systèmes de paiement basés sur des cartes de crédit ou sur d'autres moyens de facturation offrent aux clients la possibilité de payer leurs achats plus tard; en contrepartie, les émetteurs et les banques doivent s'assurer de la qualité du dossier de crédit de chaque client afin de déterminer s'ils peuvent lui faire confiance quant au paiement ***différé*** des biens ou services achetés sur Internet.

b) Délai d'encaissement

Une caractéristique très importante pour le vendeur fait référence au délai d'encaissement propre à chaque système de paiement. En effet, plus ce délai est long, plus il faut de temps pour que le vendeur puisse utiliser les revenus générés par les ventes effectuées. Certains systèmes remettent les revenus périodiquement aux vendeurs – à chaque fin de mois, par exemple. D'autres envoient un paiement au vendeur dès qu'un montant minimal prédéterminé a été atteint. D'autres encore, exigent que le vendeur effectue un retrait à partir de son propre compte. Enfin, certains systèmes basés sur des billets numériques offrent aux vendeurs un accès immédiat à l'argent gagné sur Internet, car, en étant payés d'avance, ces billets ont déjà une valeur monétaire.

c) Mode d'échange des fonds

Un système qui requiert pour chaque transaction que le client (ou le vendeur) prenne contact avec la banque ou avec une autre entité intermédiaire est un système ***en-ligne*** ou indirect, puisque les deux entités doivent toutes les deux être en ligne en même temps et que les fonds ne circulent pas directement du client au vendeur, mais doivent plutôt transiter par un intermédiaire, qu'il soit une banque ou un autre organisme. Par ailleurs, les systèmes qui permettent d'effectuer des transactions directes entre le client et le vendeur sont des systèmes ***hors-ligne*** ou directs.

Dans le premier cas, le grand avantage résulte du fait que l'émetteur ou la banque s'occupe seule de l'authentification et de la validation des messages transactionnels, et accepte ou rejette sur-le-champ une transaction; ceci confère un haut niveau de sécurité au système, car en vérifiant tout de suite chaque transaction, toute tentative d'utiliser un billet contrefait sera détectée avant la fin de la transaction. Toutefois, cette facilité engendre un coût additionnel, celui de la transmission, et introduit une étape supplémentaire dans le traitement du flux monétaire. En effet, pour toute transaction effectuée, en plus de la connexion entre un client et un vendeur, une connexion de plus – avec la banque, l'intermédiaire ou l'émetteur – doit être effectuée, ce qui engendre des bits supplémentaires (*overheads*) de transmission ainsi que des temps additionnels d'attente.

Dans le deuxième cas, l'avantage primordial découle de la capacité du système de permettre les transactions directes entre deux entités transactionnelles, sans que le contact avec une tierce entité ne soit nécessaire. Ceci non seulement diminue les délais de connexion et de transmission, mais permet aussi une très grande souplesse dans le choix de l'implantation des protocoles de communication entre les deux entités transactionnelles. L'utilité des transactions directes relève aussi de leur grande flexibilité, qui permet de les implanter et de les utiliser facilement sur tout réseau et plate-forme. Par contre, le fait que la banque ne soit pas contactée implique un risque de fraude plus élevé, et donc un coût supplémentaire de vérification, car les possibilités de contrôle de l'authenticité des pièces ou des billets numériques en dehors de la banque sont beaucoup plus limitées – étant donnée la complexité de telles opérations.

d) Convertibilité de la RM

Plusieurs systèmes prévoient la possibilité d'offrir la convertibilité de leur RM en plusieurs devises réelles. Ainsi, les systèmes basés sur les cartes de crédit permettent à leurs utilisateurs d'acheter dans n'importe quelle devise; les clients seront

facturés dans la devise locale des banques qui ont émis leurs cartes respectives. Notons aussi que tous les systèmes qui s'aligneront sur les spécifications prévues par des standards internationaux, tels que SET, pourront offrir une convertibilité limitée d'une devise à une autre dans le cadre d'une même représentation monétaire virtuelle. Toutefois, à cette date, aucun système implanté commercialement ne possède d'émetteurs mettant en circulation plusieurs devises différentes en même temps.

e) Niveau de développement

Étant donnée notre désir d'effectuer une revue quasi exhaustive des systèmes électroniques de paiement sur Internet, nous avons dû inclure des systèmes qui ne sont pas au même niveau de développement que d'autres. Si certains systèmes sont déjà exploités commercialement, d'autres se trouvent, à la date de rédaction de cet ouvrage, dans une phase de tests expérimentaux, dans un ou plusieurs projets pilotes, tandis que d'autres ne sont que des articles ou des publications de recherche, sans aucune implantation physique. Nous avons aussi regardé plusieurs systèmes en phase précoce de développement afin de bien circonscrire l'état de l'art dans les systèmes de paiement électronique sur Internet et de montrer les tendances qui s'esquissent à l'horizon.

2.5 État de l'art

Même si le commerce électronique est encore un domaine très jeune, plusieurs protocoles et systèmes électroniques de paiement sur Internet ont déjà été proposées – surtout au cours des quatre dernières années. Après avoir surveillé les différents développements dans le monde des paiements numériques, presque depuis sa

naissance, nous avons compilé et mis à jour une vaste liste de ressources électroniques contenant d'amples informations sur quasiment tous les systèmes et protocoles existants aujourd'hui.

En se basant sur la taxonomie introduite dans la sous-section 2.4.1, ainsi que sur les critères d'analyse et d'évaluation introduits dans la sous-section 2.4.2, nous proposons dans les pages qui suivent une classification générale des systèmes de paiement électronique sur Internet, processus qui permet de regrouper les systèmes ayant des caractéristiques similaires. Les résultats de la classification et de l'évaluation des systèmes étudiés seront présentés dans le Tableau 2.3, tableau permettant aussi une analyse comparative de ces outils transactionnels.

Il est important de noter ici que notre classification, analyse et évaluation, ne reposent pas exclusivement sur les affirmations des auteurs. Par exemple, le système CyberCoin, contrairement à ce que son nom semble indiquer, fonctionne plus comme des chèques – avec un nom de destinataire spécifié d'avance – que comme des pièces de monnaie. De plus, même si son auteur (la compagnie américaine **CyberCash**) l'annonce comme un système de micropaiements, nous l'avons classifié comme un système de minipaiements, étant donné que le plus petit incrément avec lequel un paiement peut être effectué est de 25 cents, ce qui ne raffine pas la granularité de la devise utilisée (le dollar US). Par ailleurs, même si plusieurs systèmes sont déjà compatibles – ou vont bientôt l'être – avec un ou plusieurs standards de paiement, tels que SET, nous avons décidé de les garder dans leur groupe initial, correspondant au modèle de sécurité et à la technologie de paiement sur laquelle ils sont basés. D'autres systèmes, qui ne sont pas inclus dans cet ouvrage, peuvent exister: soit qu'il s'agisse de recherches académiques ayant des résultats qui n'ont pas encore été publiés ou n'ont pas été largement publicisés, soit qu'ils ont disparu prématurément. Enfin, des systèmes très récents, tels que NetCents, en développement à l'**Université de Toronto**, VarietyCash, en développement à l'**Université de la Californie à San Diego**, ou X-Cash, en

développement à **Bell Labs**, n'ont pas été inclus étant donnée la jeunesse de ces systèmes et, par conséquent, le manque de documentation.

2.5.1 Classification et évaluation

Nous présentons dans cette sous-section plusieurs systèmes électroniques de paiement sur Internet, classés suivant la taxonomie introduite précédemment. Nous avons étudié en détail plus de 80 systèmes et protocoles différents ainsi que plusieurs standards transactionnels. Ces systèmes et protocoles ont été proposés par des compagnies et des universités en plusieurs pays différents, notamment aux États Unis et en Europe. La plupart des systèmes déjà implantés physiquement se trouvent (à ce jour) en phase de tests internes – alpha – ou de tests externes ou projets pilotes – bêta.

Tout d'abord, nous avons appliqué les critères de classification pour départager les différents types de systèmes de paiement. Par la suite, nous avons appliqué les critères d'analyse et d'évaluation définis précédemment. Pour faciliter la compréhension, nous allons décrire le fonctionnement de plusieurs systèmes que nous avons jugés les plus représentatifs de chaque groupe, dans chaque classe et catégorie, respectivement.

2.5.1.1 Les systèmes sans adhésion

Les systèmes de paiement électronique sans adhésion reposent sur le principe de la transaction unique. Lors d'une telle transaction, un acheteur effectue un achat auprès d'un vendeur, sans avoir besoin ni d'outils spéciaux ni d'un abonnement quelconque. Il utilise simplement son fureteur, instrument qui lui permet d'effectuer une transaction rapide, reposant sur l'utilisation d'une carte de crédit ou d'un compte de chèques et utilisant souvent l'encryptage des données personnelles et financières.

2.5.1.1.1 Le modèle «sans protection»

a) Cartes de crédit / Chèques

Le modèle «sans protection», appartenant à la catégorie des systèmes sans adhésion, est le plus simple et le plus «ancien» modèle de paiement électronique. Ce modèle utilise en fait des interfaces CGI (*Common Gateway Interface*) du protocole HTTP [Référence électronique RFCD] sur lequel le Web est basé. Une telle interface fait le lien entre le Web et le serveur sur lequel la transaction devra s'exécuter; elle est habituellement codée en utilisant un langage de programmation de haut niveau, tel que Perl ou C, mais d'autres langages, tels que le Shell Script, sont très souvent utilisés, surtout pour des applications assez simples. Notons qu'il ne s'agit pas d'un système de paiement électronique proprement dit, mais plutôt d'une méthode de transport de données personnelles et financières à des fins de prise de commande et éventuellement de livraison de produits et services. Il n'y a donc pas de produit en soi, ni de vendeur précis pour cette méthode générique.

En utilisant cette interface, le numéro de la carte de crédit (ou, rarement, le numéro de compte de chèques) des clients est demandé dans un formulaire en-ligne. Pour ce faire, le vendeur met en place un catalogue électronique contenant des pages HTML [Référence électronique RFCD], dans lesquelles il annonce et décrit sa marchandise. Après avoir sélectionné le produit ou le service désiré, l'acheteur remplit le formulaire électronique qui exige, entre autres, l'adresse postale et électronique de la personne qui commande, l'adresse d'expédition, le numéro de carte de crédit et sa date d'expiration. Les informations demandées peuvent être considérées, dans la plupart des cas, comme confidentielles et personnelles. Le transfert de cette information se fait simplement à l'aide du protocole HTTP sans aucun encryptage. La vérification du compte pour approbation se fait en-ligne ou hors-ligne en utilisant un système de vérification et de facturation de cartes de crédit.

Étant donné le fait qu'aucune mesure de protection et de sécurité n'est appliquée, mais en prenant en considération le niveau de sécurité assuré de façon inhérente par le protocole HTTP, nous considérons que le niveau de sécurité de cette méthode est faible, mais non nulle. La méthode est asymétrique; elle offre une granularité grossière et un bas niveau d'anonymat, mais une totale convertibilité.

Plusieurs sites Web offrent encore une telle méthode de paiement. Parmi ces sites, les archives du prestigieux **BusinessWeek** [Référence électronique BWAR] sont un exemple bien connu. Elles sont consultables moyennant un paiement par carte de crédit qui peut se faire à l'aide d'une interface du protocole HTTP, sans encryptage ou avec un système d'encryptage utilisant le protocole SSL. En offrant le service sans encryptage, **BusinessWeek** pourrait potentiellement rejoindre tous ses lecteurs, incluant ceux qui n'ont pas de fureteur muni de fonctions cryptographiques, capables d'effectuer l'encryptage.

2.5.1.1.2 Le modèle «avec protection»

La cryptographie constitue aujourd'hui le moyen de sécurisation le plus sûr, le moins coûteux et le plus répandu, pour un nombre croissant d'applications électroniques. Dans cette classe de systèmes sans adhésion, le standard *de-facto* en ce qui concerne la protection, est le protocole SSL [Référence électronique SSLP]. SSL est un protocole de bas niveau, développé en 1994 par **Netscape Communications**, intégré de façon transparente dans plusieurs fureteurs tels que Netscape Navigator ou Internet Explorer pour augmenter le niveau de sécurité disponible sur Internet. En plus du transfert sécuritaire des données, il permet au serveur Web et au fureteur du client de s'authentifier.

Le protocole fonctionne en deux étapes, une première étape d'authentification (*handshake*), dans laquelle le chiffre asymétrique RSA [Rivest et al.,

1978] est utilisé, et une deuxième étape, celle de l'échange de données, dans laquelle plusieurs algorithmes symétriques d'encryptage [Denning, 1982] – tels que DES, triple-DES, RC2 ou RC4 – peuvent être employés. La compagnie **Microsoft** a aussi proposé un protocole équivalent, nommé PCT, mais ce protocole ne semble pas réussir à gagner la même popularité que SSL.

a) Cartes de crédit

La compagnie américaine **IBM** offre un produit de commerce électronique appelé Net.Commerce, solution basée sur l'utilisation des cartes de crédit. Elle comprend plusieurs modules de commerce électronique – incluant un catalogue, un panier électronique, une base de données, etc.– dont celui du paiement électronique qui utilise l'encryptage à l'aide du protocole SSL. Cette solution ne s'adresse pas seulement au commerce au détail, mais aussi aux transactions interentreprises. Notons qu'au Québec, la **Librairie Garneau** utilise ce système de paiement.

Regardons comment ce système de paiement électronique fonctionne. Une fois que l'acheteur a choisi la marchandise qu'il veut se procurer, il transmet sa requête au vendeur, qui retransmet la requête de paiement à la banque. La banque vérifie le crédit de l'acheteur et renvoie une confirmation (ou infirmation, le cas échéant) au vendeur. Enfin, le vendeur, après avoir reçu la confirmation de la transaction, procède à la facturation du client et à l'expédition de la marchandise commandée.

Sur le plan de la sécurité, la disponibilité, la confidentialité et l'intégrité sont garanties grâce au protocole SSL. Par contre, le système n'assure ni l'authentification ni la non-répudiation des transactions. Pour assurer ces deux aspects, **IBM** propose IBM Payment Suite, une solution qui repose sur le protocole SET. Le système est asymétrique et offre un débit de fonds différé et une convertibilité totale de la représentation monétaire.

L'accès transparent et très ergonomique aux fonctions de communication sécuritaire des fureteurs offre à ce système un avantage incontestable, mais l'utilisation des cartes de crédit restreint son accessibilité, étant disponible seulement pour ceux qui en détiennent et seulement pour des montants de transaction suffisamment grands pour être économiquement viable – habituellement 10 $ et plus. Sans offrir la non-répudiation des transactions et tenant compte que seule la communication est protégée, le niveau de sécurité de ce système est considéré comme moyen, dans le meilleur des cas.

Notons que dans cette classe, les solutions qui relient un serveur Web commercial au réseau bancaire sont les plus répandus et les plus représentatifs de l'évolution du milieu financier ainsi que de la convergence des solutions vers l'Internet. Dans ce contexte, BuyWay et TouchLink sont deux solutions québécoises – proposées par les compagnies **MPACT Immedia / BCE Emergis** et **TouchNet**, respectivement – qui assurent une passerelle entre l'Internet et le réseau bancaire, soit par un lien Datapac entre le vendeur et sa banque ou un guichet automatique NCR (**National Cash Register**) – dans le cas de TouchLink –, soit à l'aide d'une entité intermédiaire, comme dans le cas de BuyWay.

b) Chèques

Un autre moyen de paiement, à la place des cartes de crédit, consiste à utiliser des chèques, plus précisément le numéro d'un compte de chèques; les systèmes de ce type tentent d'utiliser au maximum les transactions interbancaires existantes. C'est précisément ce que propose la compagnie américaine **OnLineCheck System** avec sa solution appelée OnLineCheck. Ce système s'adresse surtout à la vente au détail et vise principalement les usagers qui ne veulent pas utiliser leur carte de crédit ou ceux qui n'en ont pas.

Une fois qu'il a choisi la marchandise, l'acheteur remplit un formulaire électronique HTML situé sur le site Web du vendeur. Il doit notamment fournir les informations relatives à son compte de chèques et à la banque où ce compte est ouvert. L'information contenue dans ce formulaire est transmise à l'intermédiaire du système (présentement la compagnie **OnLineCheck System**) via Internet et est protégée à l'aide du système SSL.

Lors de la réception des informations, l'intermédiaire imprime une version papier du chèque. Ce chèque sera transmis par courrier régulier ou prioritaire – **FedEx** ou autre, au choix du vendeur –, soit au vendeur soit à sa banque, selon une entente préalable. L'intermédiaire envoie ensuite, par courrier électronique non-encrypté, une confirmation au vendeur, l'informant de l'envoi du chèque; ce message contient, entre autres, le nom de l'acheteur ainsi que la liste des produits et des services achetés. De la même manière, l'intermédiaire confirme à l'acheteur, par courrier électronique non-encrypté, que le chèque a été expédié; le message contient, comme le premier, le nom de l'acheteur et les produits ou les services achetés. Sur réception de la confirmation, le vendeur achemine les produits ou les services en question à l'acheteur. L'acquittement du paiement se fait, comme pour tout autre chèque, par l'intermédiaire du système bancaire.

Ainsi, la méthode employée par OnLineCheck ajoute une étape supplémentaire à la procédure de paiement par chèque bancaire, notamment celle assurée par l'intermédiaire. Le vendeur doit télécharger et installer les logiciels de vente de OnLineCheck et doit adhérer aux services de l'intermédiaire – ce qui coûte 150 $ US plus des frais de 2 $ US par chèque traité. De plus, il doit obtenir un certificat RSA et installer un serveur Web muni du protocole SSL afin d'assurer la protection de son site. En ce qui concerne la sécurité, comme pour les autres systèmes utilisant le protocole SSL, la disponibilité, la confidentialité et l'intégrité sont assurées intrinsèquement. Cependant, rien ne met l'acheteur à l'abri d'un fraudeur qui pourrait copier les

informations des chèques, étant donné que la signature n'est pas exigée et qu'aucune mesure pour assurer l'authentification ou la non-répudiation n'est en place. C'est peut-être une raison pour laquelle OnLineCheck est le seul système dans cette classe à utiliser un protocole de ce genre; l'autre système que nous avons classifié dans ce groupe est Quick-Checks.

Il faut noter, toutefois, le fait qu'une augmentation significative de l'utilisation des chèques électroniques sur Internet est prévue, surtout pour l'acquittement des factures courantes comme le téléphone, l'électricité ou le câble. Plusieurs compagnies sont en train de développer des solutions de facturation (*bill presentment*) et de paiement des factures par Internet.

Pour compléter cette analyse, regardons les autres systèmes que nous avons attribués à cette classe. Comme tous utilisent SSL, ils ont tous les mêmes caractéristiques – ou des caractéristiques très semblables. Les systèmes électroniques de paiement sur Internet, sans adhésion, basés sur le modèle «avec protection» incluent, en ordre alphabétique: BuyWay, ClearCommerce, CommerceXpert, E-money.NET, Net.Commerce, NetVerify, OnLineCkeck, Payline, Payway, Secure-Bank.Com, SecureOrder, SecurePay, SecureProcess, SecureLink, SecureTrans, TouchLink et WebCash.

2.5.1.2 Les systèmes avec adhésion

Les systèmes de paiement électronique sur Internet basés sur l'utilisation des moyens cryptographiques de protection sont très nombreux. La sécurité du transfert étant ainsi assurée, les transactions commerciales pourraient être effectuées sans autre forme d'identification ou d'authentification que ce qui est inhérent à l'utilisation des cartes de crédit ou des chèques. Cependant, ceci ne protège pas contre l'utilisation frauduleuse d'une carte de crédit volée ou perdue, ni de la retranscription des données

d'un chéquier par une personne qui n'est pas autorisée à signer des chèques. Le rôle de l'adhésion est donc d'assurer un niveau de sécurité supplémentaire et d'épargner du même coup aux clients les dangers de retransmettre leurs données personnelles et bancaires avec chaque commande.

2.5.1.2.1 Le modèle «authentification»

Comme dans le cas des systèmes sans adhésion, les systèmes qui requièrent une adhésion ont leur propre modèle «primitif» ou simpliste. Ce modèle n'est pas non plus un système de paiement proprement dit, il est basé simplement sur le protocole HTTP du Web et sur un peu d'ingéniosité. Le modèle utilise la notion d'authentification simple des utilisateurs, qui ont préalablement dû s'enregistrer auprès des vendeurs utilisant un tel système.

a) Mots de passe / *Cookies*

Un premier groupe dans cette classe utilise uniquement le protocole HTTP. Lors de l'adhésion, un acheteur potentiel enregistre plusieurs informations personnelles, telles que son nom et adresse, le numéro de sa carte de crédit ainsi que la date d'expiration de cette carte, un pseudonyme et un mot de passe, et certaines options de livraison. Cet enregistrement initial se fait à l'aide de formulaires électroniques HTML et la transmission des données peut se faire – selon le site et le choix de l'usager – en clair ou en mode protégé, à l'aide des moyens cryptographiques, tels que SSL. Après avoir effectué l'enregistrement et le choix du mot de passe, l'acheteur peut commencer à magasiner.

Le principe d'un tel protocole de paiement est simple et facile à implanter et gérer, tant pour les vendeurs que pour les clients. Malheureusement les désavantages de l'utilisation des mots de passe sont de plus en plus évidentes. Les utilisateurs n'utilisent

qu'un petit nombre de caractères pour former leur mot de passe ou prennent un nom commun une date du calendrier. Une fois qu'une tierce personne a obtenu un mot de passe, frauduleusement ou non, elle peut effectuer toutes les opérations financières au nom de l'usager original, car aucun autre moyen d'authentification de cette personne n'est utilisé.

Certains vendeurs envoient aux utilisateurs, à la fin du processus d'enregistrement, un ou plusieurs *cookies* qui serviront à les identifier lors des visites subséquentes. Lors d'une transaction, l'acheteur est authentifié par le vendeur par son mot de passe ou par ce *cookie* – qui peut, pour un peu plus de sécurité, avoir une date d'expiration.

Ce modèle n'est pas représenté par une solution d'une compagnie en particulier, il est constitué plutôt d'une méthode de paiement que d'un système donné. Un site bien connu qui utilise cette méthode est le site de la librairie virtuelle **Amazon.com** [Référence électronique AMZN].

b) «Dépôt légal»

Un deuxième groupe de cette classe contient, lui aussi, un seul système: SafePurchase. Ce système n'utilise, lui non plus, des moyens de protection par encryptage. Il emploie la notion de «dépôt légal» pour lui servir de mécanisme permettant l'identification et l'authentification de l'acheteur à des fins de prise de commande ou de transfert de données.

Le système nécessite l'ouverture d'un compte chez l'intermédiaire – pour le moment, la compagnie **SafePurchase** est le seul intermédiaire à offrir ce système. Les données personnelles et financières sont transmises via l'Internet ou par des moyens alternatifs – tels que le courrier électronique ou le téléphone.

Après s'être inscrit, l'acheteur peut aller magasiner sur le Web. Une fois le choix du produit ou du service effectué, l'acheteur indique au vendeur son intention de payer avec le système de dépôt légal de **SafePurchase**. Il dépose dans son compte SafePurchase le montant de la transaction en utilisant un chèque bancaire ou un mandat postal – envoyé par la poste – ou un numéro de carte de crédit – transmis par téléphone. Une fois le montant reçu, c'est à **SafePurchase** d'informer le vendeur de la disponibilité de l'argent à son intention. Le vendeur peut alors livrer la marchandise à l'acheteur et transmet à **SafePurchase** le numéro d'envoi. L'acheteur bénéficie d'un délai de deux jours pour examiner la marchandise et la retourner dans le cas où il ne serait pas satisfait, sinon, **SafePurchase** libère l'argent au nom du vendeur.

Seul l'acheteur doit posséder un compte chez l'intermédiaire, le vendeur, n'a besoin que d'une adresse de courrier électronique ou d'un numéro de télécopieur; le magasinage peut donc se faire aussi par catalogue. Notons le fait que cette solution est orientée vers les transactions interentreprises; elle est une des seules à donner à l'acheteur la possibilité de retourner la marchandise achetée. Par contre, ce système n'utilise aucun moyen de sécurisation cryptographique et la plupart des sous-critères de protection ne sont pas remplis; nous concluons alors qu'il offre un faible niveau de sécurité. Au lieu d'être rapide et intuitive, une transaction peut durer plusieurs jours et un vendeur n'est pas tenu d'accepter ce type de transaction. Cependant, n'importe quel vendeur peut effectuer des ventes à l'aide de ce système, sans même s'y inscrire.

2.5.1.2.2 Le modèle «débit-crédit»

Le modèle «débit-crédit» regroupe le plus grand nombre de systèmes électroniques de paiement, englobant trois groupes et un sous-groupe. Chaque groupe apporte des solutions intéressantes, soit pour éliminer la nécessité de donner son numéro de carte de crédit en-ligne – comme c'est le cas du système FirstVirtual – ou pour trouver une alternative à l'échange de documents sur papier – comme le système

BankNet qui sera décrit dans les pages suivantes –, soit pour corriger certaines faiblesses du protocole de protection SSL – comme le fait le système CyberCash – ou pour assurer l'authentification des intervenants et éliminer la répudiation des transactions – le cas du sous-groupe SET.

a) NIP / Mots de passe

Un pionnier du commerce électronique est la compagnie américaine **FirstVirtual** qui a lancé en 1994 ses produits logiciels de paiement électronique. Le système FirstVirtual utilise un système en-ligne, asymétrique, qui transmet lors de chaque transaction le NIP de l'acheteur. C'est un des seuls systèmes à ne pas utiliser d'outils d'encryptage.

Pour ouvrir un compte et adhérer ainsi au système, l'acheteur donne son numéro de carte de crédit par téléphone à la compagnie **FirstVirtual**, en utilisant un numéro sans frais. En retour, il reçoit son NIP qui va lui servir pour s'identifier et payer. De leur côté, les vendeurs doivent aussi s'enregistrer et télécharger des logiciels de vente, accompagnés de plusieurs scripts, qui doivent être installés sur leurs serveurs Web. Deux types de comptes vendeurs sont disponibles; selon le type de compte ouvert, un délai de 4 à 91 jours est nécessaire avant que le compte du vendeur soit crédité. Des frais d'adhésion et un pourcentage s'appliquent pour toute transaction. À ce jour, plus de 1200 vendeurs acceptent des paiements utilisant ce système.

Dans le site d'un marchand participant, l'acheteur choisit sa marchandise et donne au vendeur son NIP. Ce NIP est tout simplement un code personnel du client, qui, en l'utilisant, accepte les conditions d'achat, et donc le transfert de fonds. Le vendeur envoie les données de la transaction accompagnées du NIP de l'acheteur à **FirstVirtual**, qui vérifie le message et envoie à l'acheteur, par courrier électronique, une demande de confirmation de la transaction. L'acheteur confirme ou infirme la

transaction par courrier électronique. Dans le cas d'une confirmation de la transaction, la carte de crédit dont l'acheteur a donné le numéro par téléphone, est facturée par **FirstVirtual** hors-ligne, en mode différé et sans utiliser l'Internet. En même temps, **FirstVirtual** envoie, toujours par courrier électronique, une confirmation finale au vendeur, qui peut alors livrer la marchandise à l'acheteur.

Une particularité intéressante de ce système consiste dans sa capacité de permettre aux acheteurs d'essayer un produit avant de l'acheter, grâce à l'application d'une politique de remboursement. Par contre, le NIP peut être utilisé seulement accompagné d'un protocole de confirmation de chaque transaction par courrier électronique. Le verdict final de l'acheteur quant à l'achat d'un produit est donc envoyé par courrier électronique, en mode différé, et ainsi, la transaction, dans son ensemble, ne s'effectue pas immédiatement.

Du point de vue sécurité, le système FirstVirtual n'assure ni la disponibilité ni la confidentialité ni l'intégrité des informations de la transaction, étant donné qu'aucun moyen cryptographique n'est utilisé. Toute commande peut alors être interceptée. Mais comme la sécurité du numéro de la carte de crédit n'est pas directement compromise, et que l'authentification est assurée par le NIP, on peut considérer le niveau de sécurité de FirstVirtual comme étant moyen. Notons enfin que le groupe des systèmes basés sur un NIP ou mot de passe inclut, en plus de FirstVirtual, les systèmes Internet Dollar et WebCharge.

b) Chèques électroniques

Le deuxième groupe en importance appartenant à ce modèle est celui des systèmes employant des chèques électroniques. Un exemple d'un tel système est la solution britannique BankNet, qui, contrairement à la solution proposée par le système OnLineCheck, ne transmet pas les informations figurant sur un chèque bancaire en les

reproduisant dans un formulaire qui sera imprimé. La compagnie **BankNet** – qui s'annonce comme une «banque sur Internet», offrant presque tous les services qu'une banque ordinaire offre – propose un produit, au stade de développement bêta, qui comprend un logiciel et des comptes bancaires.

Dans ce système, l'acheteur et le vendeur doivent tous les deux avoir un compte avec **BankNet** – entité qui joue, à la fois, le rôle de banque et d'intermédiaire. L'acheteur doit utiliser un fureteur possédant des capacités cryptographiques pour magasiner, ainsi qu'un logiciel appelé WorkHorse – disponible présentement pour le système d'opération Windows 3.1 seulement – qui sert à l'authentification, notamment pour générer une paire de clés asymétriques, une clé publique et une clé privée, et pour effectuer des signatures numériques. Après avoir généré cette paire de clés, l'acheteur s'enregistre auprès de **BankNet** en fournissant sa clé publique et en ouvrant un compte. Au moment de l'enregistrement, l'acheteur peut imposer certaines limites aux transactions qu'il pourrait effectuer, telles que le montant limite pour chaque transaction, le montant total transigible pour une semaine ou le temps de vie de sa clé publique. Une fois enregistré, pour effectuer une transaction l'acheteur choisit sa marchandise et envoie sa commande au vendeur en incluant un chèque électronique dans son message. Notons le fait que le vendeur n'a pas besoin de connaître la clé publique de l'acheteur; ceci implique le fait que la vérification de la signature numérique incombe à la banque et que, sans cette clé publique, le vendeur ne peut pas vérifier la signature de ses clients.

Pour accepter des chèques, le vendeur doit posséder, lui aussi, un compte **BankNet**, ainsi qu'un site Web muni d'un système de commerce électronique – qui ne relève pas de la solution BankNet. Après avoir reçu le paiement sous forme de chèques électroniques BankNet, le vendeur achemine la marchandise à l'acheteur et dépose ses chèques à la banque qui s'occupe du transfert entre le compte de l'acheteur et celui du vendeur.

En ce qui concerne la sécurité, cette solution permet au vendeur l'emploi du protocole SSL, assurant ainsi une bonne protection des transactions. Toutefois, si le serveur du vendeur n'utilise pas ce protocole, il n'y a alors aucune protection au niveau de la disponibilité ou de la confidentialité. Par contre, en utilisant un logiciel distinct pour effectuer des signatures numériques, le système assure l'intégrité des messages, l'authentification des intervenants et la non-répudiation des transactions. Précisons le fait que, pour des «raisons de sécurité», la **Banque d'Angleterre** a demandé à **BankNet** de limiter les transactions à 50 £. Notre conclusion est que la sécurité assurée par ce système de chèques électroniques peut être considérée comme forte.

D'autres systèmes indirects offrent des solutions semblables: ainsi, le système CheckFree permet d'effectuer des transactions, pour lesquelles le client reçoit une facture mensuelle payable à CheckFree, qui, en retour, payera les vendeurs. Le protocole ressemble fortement aux autres systèmes de chèques électroniques. Electronic Check ou E-Check de **Financial Services Technology Consortium**, appuyé, entre autres, par **BankBoston**, se veut l'équivalent électronique d'un chèque ordinaire sur papier, avec ses avantages – mais aussi ses inconvénients. Le système est en-ligne, asymétrique et utilise des numéros de compte encryptés comme RM transmise sur le réseau. Comme l'implication des banques doit être – tout comme dans le cas des chèques ordinaires – très grande, le système est toujours à l'état de projet.

D'une manière similaire, mais en utilisant un système de protection Kerberos[3] pour l'authentification des signatures numériques, l'**Université de la Californie du Sud** propose NetCheque, un système de chèques électroniques bien intégré au Web à l'aide des formulaires électroniques HTML. Notons, pour conclure,

[3] Kerberos [Référence électronique KRBR] est un système d'authentification développé au **MIT**, aux États Unis. Il utilise un serveur de sécurité permettant au client de s'authentifier sans transmettre d'informations confidentielles et encrypte les échanges subséquents. Le système est basé sur l'algorithme symétrique d'encryptage DES.

que les systèmes de paiement appartenant à ce groupe incluent, par ordre alphabétique: AIMP, BankNet, CheckFree, CyberCoin, E-Check, NetCheque, NetChex, NetFare, Redi-Check, SNPP et Vishnu.

c) Facturation / Cartes de crédit

Le groupe le plus important dans la classe de modèles «débit-crédit» est celui des systèmes de paiement basés sur la facturation et sur les cartes de crédit. Dans ce groupe, un des systèmes les plus répandus à l'heure actuelle est le système CyberCash, offert par la compagnie du même nom, système adopté déjà par plusieurs entreprises ainsi qu'à l'état de test ou projet pilote par plusieurs banques telles que **Wells Fargo**, **American Express** ou **First USA**. La **Banque Nationale du Canada** détient aussi une licence de CyberCash qu'elle commercialise sous le nom de SecurNat.

Avec un portefeuille virtuel muni d'une interface graphique et en utilisant l'encryptage à clés publiques, ce qui permet d'augmenter substantiellement le niveau de sécurité, CyberCash est un système en-ligne, asymétrique, qui débite l'acheteur par l'intermédiaire de sa carte de crédit. Il s'agit d'une solution qui corrige plusieurs faiblesses des systèmes basés sur le protocole SSL.

Afin d'utiliser cette solution de paiement, l'acheteur télécharge son portefeuille électronique et adhère au système en enregistrant sa carte de crédit auprès de **CyberCash** ou d'un autre détenteur d'une licence. Ce portefeuille lui permet non seulement de s'identifier et de s'authentifier, mais aussi de garder les traces des toutes les transactions. Pour magasiner, l'acheteur choisit sa marchandise sur le site Web du vendeur en suivant les procédures d'achat du magasin; son portefeuille virtuel est activé automatiquement avant le paiement, procédure qui est effectuée en transmettant au vendeur un message encrypté contenant, entre autres, le numéro de sa carte de crédit. Le vendeur retransmet ce message à la banque, sans avoir accès au numéro de la carte – qui

reste illisible, étant encrypté avec la clé publique de la banque. Suite à l'autorisation de la banque, le vendeur livre au client la marchandise achetée.

Pour vendre sur Internet en utilisant ce système de paiement, le vendeur doit acheter une licence puis télécharger et installer un logiciel de vente sur son serveur Web. Il doit ensuite adhérer et ouvrir un compte auprès de **CyberCash** ou d'autres détenteurs d'une licence. Notons que cette licence peut être exclusive, empêchant le vendeur d'offrir aux acheteurs le choix d'utiliser d'autres moyens de paiement électronique.

En ce qui concerne la protection, le système emploie des moyens d'encryptage à clés publiques, qui assurent une très forte sécurité. C'est peut être une des raisons pour laquelle CyberCash est l'un des systèmes ayant la plus grande pénétration commerciale aujourd'hui. D'autres systèmes relativement récents tentent de s'inspirer des techniques de CyberCash; ainsi, par exemple, une solution française appelée Klebox, possède des caractéristiques très similaires.

Le système ClickShare, par ailleurs, effectue des «transferts de frais» entre un acheteur et le site Web d'un vendeur, de façon indirecte, en envoyant aux clients une facture périodique pour les achats effectués. Le montant minimal d'une transaction doit dépasser 10 cents et aucune confidentialité n'est assurée, le serveur ayant une liste complète des noms des clients. NetBill [Cox et al., 1995], proposé par les chercheurs de l'**Université Carnegie Mellon**, est plutôt un environnement transactionnel, qui prend le rôle d'intermédiaire entre le client et le vendeur. Le client demande le prix d'un bien et initie la transaction, qui sera effectuée par l'intermédiaire d'un serveur spécial permettant l'authentification et la validation du paiement.

Enfin, certaines solutions, comme Web900, exigent l'utilisation d'un numéro téléphonique à frais, de type 1-900. Lors de l'appel, l'acheteur est facturé sur

son compte de téléphone ou sur sa carte de crédit et reçoit en échange un mot de passe lui permettant d'accéder à la marchandise numérique qu'il vient d'acheter. Une solution semblable sera implantée bientôt au Canada par la compagnie **BCT.Tellus** en collaboration avec **eCHARGE**.

Beaucoup d'autres systèmes sont offerts aujourd'hui dans ce groupe. La plupart sont soit en phase commerciale, soit sur le point de l'être. Les systèmes que nous avons placés dans ce groupe incluent, par ordre alphabétique: ACC, BlueMoney Network Wallet, ClickShare, Cybank, CyberCash, eCHARGE, Evend, InterCoin, iKP, Klebox, Neosphere Web TollBooth, NetBill, Pay2See, Web900 et ZipLock.

c1) Le sous-groupe SET

Face à la forte et très rapide croissance du nombre de paiements électroniques utilisant les cartes de crédit sur Internet, un besoin de plus en plus évident est apparu: celui d'introduire des standards permettant l'emploi d'environnements transactionnels commerciaux à normes uniformisées. L'initiative [encore expérimentale] ayant connu le plus grand succès à ce jour est SET – un standard qui vise justement les transactions utilisant les cartes de crédit, standard qui attend [encore] son entrée dans la phase commerciale depuis quelques années déjà.

Le nombre de systèmes qui utilisent SET a crû assez rapidement dans un très court laps de temps. Ainsi, tous ces systèmes – tous en phase de tests pilote ou de tests bêta – forment leur propre sous-groupe (le sous-groupe SET) dans le cadre du groupe de systèmes basés sur la facturation et les cartes de crédit. Ayant le support de grandes compagnies comme **VISA** et **MasterCard**, cette solution est attendue comme une solution des plus prometteuses. Mais de longs délais, des dates limites repoussées à plusieurs reprises, ainsi que la critique concertée de plusieurs analystes connus ont semé le doute dans l'esprit des consommateurs, de plus en plus habitués à utiliser le protocole

SSL. Malgré tous les efforts et les annonces consacrés à ce protocole depuis bientôt trois ans, il n'y a toujours pas d'implantation commerciale disponible à l'heure actuelle.

Cependant, précisons le fait que la plupart des systèmes de paiement disponibles commercialement aujourd'hui annoncent d'une façon ou d'une autre leurs intentions de se rendre compatibles avec SET dans leurs prochaines versions. Mentionnons aussi le fait qu'une extension de SET, connue sous le nom de C-SET (*Chip-Secure Electronic Transaction*) a été développée pour être utilisée avec les cartes intelligentes.

Par ailleurs, **IBM** avait proposé iKP (*Internet Keyed Payments*), une famille de protocoles sécuritaires de paiement, combinant les concepts de clés privés et clés publiques. Le paradigme transactionnel qui avait été utilisé impliquait l'existence de tierces parties pour compléter une transaction. Avec ce protocole, les clients placent un ordre en utilisant l'Internet, mais le paiement est effectué sur un réseau privé. Notons qu'**IBM** s'est rallié récemment à l'initiative SET. Suite à cette décision, **IBM** a crée une nouvelle solution de paiement électronique sur Internet, connue sous le nom de IBM Payment Suite, qui repose sur ce standard, et constitue une des premières implantations de ce protocole transactionnel.

Pour comprendre le fonctionnement de ce système nous devons regarder de plus près le fonctionnement de SET. Dans ce système avec adhésion, il y a quatre entités transactionnelles: l'acheteur, le vendeur, l'intermédiaire et la banque; les banques sont les premières entités qui doivent adhérer; les acheteurs doivent alors posséder une carte de crédit émise par une des banques membres du système. Chaque entité transactionnelle doit se procurer des certificats numériques émis par une autorité de certification qui est, en général, la banque.

L'acheteur télécharge son portefeuille virtuel offert par la banque émettrice de sa carte de crédit et adhère en installant son certificat numérique dans son portefeuille virtuel. Pour magasiner, l'acheteur visite le site Web d'un vendeur et choisit sa marchandise. Le portefeuille virtuel de l'acheteur s'active automatiquement, comme dans le cas de CyberCash, avant le paiement. L'acheteur entre alors son mot de passe – servant à protéger son portefeuille virtuel – et révise les détails de la transaction à payer. Une fois la transaction approuvée, son portefeuille envoie au vendeur la requête d'achat signée numériquement ainsi que le numéro de sa carte de crédit, encrypté avec la clé publique de l'intermédiaire.

De cette façon, le vendeur n'a pas accès aux informations confidentielles de l'acheteur, elles sont retransmises immédiatement à la banque – à l'aide de l'intermédiaire – accompagnées d'une requête d'autorisation pour la transaction en cours. La banque envoie une réponse au vendeur, à l'aide de l'intermédiaire; si la transaction a été approuvée, le vendeur peut alors livrer la marchandise à l'acheteur, et lui envoyer un reçu numérique contenant les détails de la transaction.

Ce protocole est à la base du système IBM Payment Suite, solution comprenant quatre ensembles de logiciels, un pour chaque entité transactionnelle. Ainsi, l'acheteur doit télécharger et installer le logiciel Consumer Wallet, doit adhérer et ouvrir un compte auprès d'une banque participante, et doit obtenir un certificat numérique. Le vendeur doit acheter et installer le logiciel de vente Payment Server, doit adhérer et ouvrir un compte auprès d'une banque participante, et doit obtenir un certificat numérique. L'intermédiaire doit acheter une licence, puis acheter et installer le logiciel Payment Gateway; il est probable que le rôle d'intermédiaire sera joué assez souvent par les banques elles-mêmes. Enfin, les banques joueront aussi le rôle d'autorités de certification pour certifier les intermédiaires, les vendeurs et les acheteurs. Pour ce faire, elles devront acheter une licence, installer un (ou plusieurs) serveur(s) ainsi que le

logiciel Payment Registry, logiciel permettant de traiter des paiements SET ainsi que d'émettre les certificats numériques.

Sur le plan de la sécurité, le système assure une protection très forte. La disponibilité et la confidentialité sont assurées par l'encryptage à clés publiques, alors que l'intégrité des informations, l'authentification des intervenants et la non-répudiation des transactions sont assurées par l'utilisation des signatures numériques.

Tous les autres systèmes qui implantent le protocole SET ont, évidemment, les mêmes caractéristiques. Ces systèmes, faisant partie du sous-groupe SET, incluent: e-Comm, GlobeSet, IBM Payment Suite, ITP Wallet, SecureWeb Payments, VeriFone et WebWallet.

2.5.1.2.3 Le modèle «comptant»

a) Pièces numériques / Billets virtuels

Le modèle «comptant» substitue à l'argent réel de l'argent électronique ayant la forme de cartes intelligentes ou de fichiers binaires contenant des pièces numériques ou des billets virtuels. Ce modèle est très bien représenté par le système eCash de la compagnie hollandaise **DigiCash**. Le système eCash est une implantation à la fine pointe de la technologie d'un algorithme introduit par David Chaum [Chaum, 1981], [Chaum et al., 1990], [Chaum, 1991].

eCash est un système en-ligne, symétrique, qui emploie des pièces numériques comme moyen de transfert de valeurs [Chaum et Brands, 1997]. Chaque pièce a une valeur nominale, un numéro de série et une signature numérique de la banque émettrice. Il s'agit de fichiers numériques que l'on achète avec de l'argent réel –

moyennant, par exemple, un transfert bancaire, une carte de crédit ou un chèque certifié – et que l'on échange lors de chaque achat contre des produits et services

La symétrie du système constitue un de ses aspects très intéressants: le même logiciel est employé tant par l'acheteur que par le vendeur, et ainsi, la distinction entre les deux entités s'estompe. De plus, le protocole supporte aussi bien les transactions en-ligne par liaison TCP/IP que les transactions en temps différé par courrier électronique – transactions qui, par contre, ne sont validées qu'après un contact avec la banque.

Pour adhérer au système, l'acheteur enregistre hors-ligne ses données personnelles et ouvre un compte auprès d'une banque ou d'un autre émetteur participant, en remplissant plusieurs formulaires sur papier qui doivent être envoyés par la poste. Une fois le compte ouvert – opération qui peut durer plusieurs jours – l'acheteur télécharge et installe un logiciel qui lui servira de porte-monnaie électronique. Il achète des pièces numériques eCash avec de l'argent réel, en déposant dans son compte une somme qui est convertie en unités eCash pouvant être transférées dans son porte-monnaie virtuel. Une fois retiré, cet argent électronique est stocké sur le disque dur de l'ordinateur de l'acheteur et peut être transporté sur une disquette, par exemple, pour utilisation à partir d'autres ordinateurs – s'ils sont munis du même logiciel transactionnel.

Le vendeur suit la même procédure d'adhésion, mais doit installer quelques scripts de plus sur son serveur Web. En ce qui concerne les banques émettrices, elles doivent acheter une licence auprès de la compagnie **DigiCash** et installer les logiciels afférents. Précisons que les pièces virtuelles émises par des émetteurs différents ne sont pas nécessairement compatibles et interchangeables.

Pour réaliser une transaction, le porte-monnaie électronique de l'acheteur contacte le porte-monnaie électronique du vendeur et transmet plusieurs pièces totalisant le montant de la transaction. Le logiciel du vendeur contacte immédiatement la banque et lui envoie le paiement reçu. La banque vérifie chaque pièce sur-le-champ, et, le cas échéant, dépose le montant de la transaction dans le compte du vendeur, tout en lui envoyant un reçu. Finalement, le vendeur envoie la marchandise et un reçu électronique au client.

Le système entier a été conçu en portant une attention particulière sur la facilité de l'implanter, de l'intégrer et de l'utiliser avec le Web. Pour ce qui est de la sécurité, eCash peut être considéré comme étant un système offrant une sécurité très forte. Les moyens d'encryptage à clés publiques utilisés assurent la disponibilité et la confidentialité de l'information, alors que les signatures numériques assurent l'intégrité de l'information, l'authentification des intervenants et la non-répudiation des transactions. De plus, en employant la notion de «signatures aveugles» – notion basée sur un «facteur d'aveuglement» [Chaum, 1983], à l'aide duquel le numéro de série d'une pièce peut être «caché» par multiplication avant que la banque la signe – les usagers s'assurent que leurs pièces numériques ne sont pas retraçables, garantissant ainsi un haut niveau d'anonymat. Le système a d'ailleurs été déjà implanté commercialement, ainsi que dans le cadre de plusieurs tests pilote par plusieurs banques, telles que la **DeutscheBank** d'Allemagne ou la **BankAustria** d'Autriche.

Dans le même ordre d'idées, un protocole hors-ligne très intéressant a été proposé par le chercheur hollandais Niels Ferguson [Ferguson, 1993], protocole symétrique véhiculant des pièces de monnaie virtuelle. Lors d'une transaction, les usagers ne sont pas contraints à contacter la banque émettrice, les pièces pouvant résider sur une simple disquette.

La particularité du système est que les pièces ont une durée de vie très limitée: en effet, elles ne peuvent être utilisées qu'une seule fois, lors d'une seule transaction. Une fois reçues, les pièces ne peuvent plus être dépensées par l'usager mais doivent être déposées auprès de la banque émettrice – mais pas nécessairement immédiatement.

Finalement, dans le même groupe, on retrouve les cartes-à-puce, ou cartes intelligentes, bien connues en Europe depuis plusieurs années déjà. Utilisées principalement comme cartes bancaires et téléphoniques, elles commencent à trouver une nouvelle utilisation comme moyen ergonomique de paiement sur Internet [Brands, 1995a]. Un des seuls systèmes de paiement électronique sur Internet à utiliser des cartes intelligentes est le système britannique Mondex, produit par la compagnie du même nom. Ce système est déjà en phase de tests bêta, étant implanté expérimentalement en Angleterre depuis quelques années, en Ontario depuis 1996, et, à partir de l'automne 1999, au Québec, à Sherbrooke.

Ce système symétrique est basé sur un microprocesseur (Hitachi H3/310, par exemple), protégé par fabrication contre toute tentative d'interférence de l'extérieur, implanté dans une carte de plastique ayant les dimensions d'une carte de crédit. Il contient essentiellement un compteur qui est décrémenté à mesure que l'argent se trouvant sur la carte est dépensé. Des mécanismes cryptographiques pour les communications avec l'extérieur de la carte sont aussi intégrés au système.

En adhérant au système, l'acheteur (ou le vendeur) reçoit une carte Mondex et peut, de façon optionnelle, se munir d'un «portefeuille Mondex» – appareil miniaturisé, surtout utile aux vendeurs, permettant la lecture et le transfert de fonds entre deux cartes. L'acheteur paie ses achats en utilisant sa carte qui sera débitée par tout appareil muni d'un lecteur de cartes Mondex, tel qu'une caisse automatique ou un téléphone. L'argent présent sur les cartes peut, à tout moment, être déposé à la banque,

reconverti en argent réel et transféré dans le compte bancaire de l'acheteur. Pour recharger sa carte, l'usager transfère de l'argent sur celle-ci à partir de son compte bancaire (ou d'une autre carte), en utilisant un téléphone, un guichet bancaire ou un autre appareil muni d'un lecteur de cartes intelligentes.

Tel que conçu à l'heure actuelle, Mondex n'est pas utilisable directement sur des réseaux numériques publics. Cependant, la compagnie britannique **Mondex**, va permettre l'utilisation sur Internet de sa carte de paiement, à l'aide du protocole SecureBuy de la compagnie américaine **AT&T**. Employant des lecteurs spéciaux, branchés chacun sur un port sériel de communication d'un ordinateur, deux cartes Mondex pourront communiquer directement pour effectuer des transactions sécuritaires. De cette façon, le système permet le paiement des achats non seulement par Internet, mais aussi par téléphone, pourvu que les entités transactionnelles participantes soient munies de l'équipement matériel nécessaire.

En ce qui concerne la protection, le système Mondex offre un haut niveau d'anonymat et peut être considéré comme un système à forte sécurité. Les sous-critères de disponibilité, de confidentialité, d'intégrité et d'authentification sont assurées par des techniques cryptographiques. Seul le sous-critère de non-répudiation n'est pas respecté, car un usager pourrait prétendre ne pas être celui qui a effectué une transaction, la carte intelligente étant «au porteur», sans identification de son propriétaire. Notons aussi que l'investissement qu'un lecteur de cartes implique pour un vendeur, et surtout pour les clients, ne pourra avoir comme résultat que de désavantager ce système par rapport à ceux qui reposent sur une approche purement logicielle.

Un autre système semblable, décrit par un autre chercheur hollandais, Stefan Brands [Brands, 1994a], [Brands, 1995b], utilise toujours une carte intelligente, mais il est conçu spécifiquement pour être utilisé sur Internet. Le compteur est surveillé cette fois-ci par un «témoin» qui se trouve dans le microprocesseur lui-même –

microprocesseur résistant aux altérations physiques. Le témoin empêche, en utilisant des mécanismes cryptographiques, toute manipulation frauduleuse du compteur et s'assure du bon fonctionnement de la partie interne au microprocesseur du système – surtout pour les transactions hors-ligne. Même si cette méthode n'est pas implantée physiquement, elle reste une idée intéressante surtout comme modèle d'intégration des supports matériels aux supports logiciels.

Étant donnée la complexité nécessaire pour assurer un fonctionnement adéquat des systèmes basés sur l'argent virtuel, la plupart des protocoles proposés sont seulement à l'état de travaux de recherche décrits dans des publications, sans aucune implantation physique. De plus, certains n'ont même pas de nom; ainsi, nous les avons identifiés par le nom de leurs auteurs, et nous les avons mis entre guillemets. Le groupe de systèmes basés sur des pièces numériques et billets virtuels inclut: "Brands", "Camenisch, Piveteau & Stadler", "Chan, Frankel & Tsiounis", eCash, "Ferguson", FOLC, IVC / GlobeID, "Jakobsson & Yung", "Lysyanskaya & Ramzan", Magic Money, Mondex, NetCash, Payme et PC Pay.

a1) Le sous-groupe des micropaiements

L'argent virtuel a donné naissance récemment à un nouveau concept économique, celui des microtransactions. L'exemple le plus souvent utilisé pour illustrer le besoin pour ce type de transactions est celui de la consultation des moteurs de recherche sur Internet ou, alternativement, la consultation des bases de données, la lecture de journaux numériques, etc. Les nouveaux produits et services que l'on peut acheter sur Internet peuvent parfois avoir une valeur minime, mais non-négligeable, surtout lorsque le volume de transactions est élevé. Pour répondre à de tels besoins, il s'agit de créer des systèmes de paiement capables de gérer de petites sommes qui coûteraient plus cher en frais bancaires si on les payait, par exemple, par carte de crédit.

Ce modèle microtransactionnel est un sous-groupe appartenant au groupe des systèmes basés sur les pièces numériques et les billets virtuels, qui relève directement du modèle «comptant». Évidemment, ce nouveau type transactionnel ouvre de nouvelles perspectives et opportunités entrepreneuriales pour les microtransactions à très faible valeur.

Même si plusieurs systèmes ont été proposés récemment, seul MilliCent, développé par la compagnie américaine **Digital**, a dépassé la phase de recherche. Aujourd'hui en phase de tests expérimentaux et de projets pilote – parmi lesquels le site du **Musée canadien des civilisations** à Hull – le système permet de transiger des montants aussi petits qu'une dizaine de cent (américain) et utilise des coupons numériques, émis par chaque vendeur, qui peuvent être achetés et échangés auprès des courtiers virtuels.

Le système est en-ligne, asymétrique et véhicule des coupons numériques à l'aide d'un protocole très bien optimisé pour un gros volume de transactions à faible coût. L'acheteur doit utiliser un porte-monnaie virtuel et un logiciel appelé MilliCent Wallet, qu'il doit télécharger et installer.

Chaque vendeur participant émet ses propres coupons pouvant ainsi les vérifier seul, donc beaucoup plus rapidement, puisqu'il en est l'émetteur. L'acheteur achète les coupons virtuels auprès d'un «courtier MilliCent» avec de l'argent réel en payant avec sa carte de crédit, ou par chèque. Pour adhérer au système, le vendeur doit télécharger et installer un logiciel de vente, s'inscrire auprès d'un courtier MilliCent et émettre un certain nombre de coupons virtuels, qui doivent être envoyés au courtier pour être vendus. Enfin, le courtier doit acheter une licence auprès de la compagnie **Digital** et installe un serveur spécial MilliCent et les logiciels afférents.

Notons le fait que les coupons sont acceptés seulement auprès de leur émetteur, ce qui en réduit la portée et en complique l'usage du système – lorsque le nombre de vendeurs augmente, il devient difficile de gérer dans son portefeuille des milliers de types de coupons émis par des milliers de commerçants différents. Par contre, ceci justifie l'existence des courtiers MilliCent, qui échangent les coupons des différents émetteurs entre eux, suivant un taux d'échange. Périodiquement, les courtiers MilliCent compensent les vendeurs, en fonction du nombre des coupons vendus, et donc de l'argent encaissé pour les coupons de chaque émetteur.

Sur le plan de la sécurité, le système n'utilise pas de moyens d'encryptage et ne remplit pas la totalité des sous-critères de protection – notamment, la disponibilité et la confidentialité des informations ne sont pas assurées. Toutefois, des signatures numériques sont utilisées pour l'intégrité de l'information, l'authentification des intervenants et pour assurer la non-répudiation des transactions. L'accès au porte-monnaie peut être restreint à l'aide d'un mot de passe. Donc, nous pouvons conclure que le système offre une sécurité moyenne.

Comme nous l'avons mentionné, aucun système microtransactionnel n'est arrivé pour le moment à l'étape commerciale. Cependant, l'intérêt montré par plusieurs grandes compagnies et certaines banques laisse entrevoir un changement possible de cette situation. Les systèmes de paiement du sous-groupe des micropaiements incluent: Belle Micro Payment System, MicroMint, MilliCent, MiniPay, MPTP, NetCard, PayWord, SOX, SubScrip et SVP.

2.5.2 Analyse et synthèse

Le Tableau 2.3 présente une synthèse des systèmes décrits précédemment de façon à permettre une meilleure comparaison et analyse. Rappelons qu'une liste quasi

exhaustive de ressources électroniques – comprenant les adresses URL pointant vers les sites Web de certains systèmes ou, sinon, vers des documents en format électronique qui les décrivent – est incluse dans une section distincte de la bibliographie. Des liens vers d'autres informations et recherches pertinentes sont aussi incluses [Référence électronique AIRR].

En synthétisant les résultats de notre analyse comparative, nous pouvons faire ressortir les forces et les faiblesses de chaque groupe de systèmes. Ceci nous permettra de tirer plusieurs conclusions sur lesquelles nous allons baser, dans le chapitre suivant, notre analyse des besoins d'un nouveau système transactionnel.

Ainsi, les transactions en-ligne, étant vérifiées tout de suite, sont plus sécuritaires et se prêtent mieux aux transferts importants de valeur. Les systèmes hors-ligne sont plus commodes, plus rapides en termes de transfert final, acquittement et clearing de fonds. Dans ces systèmes l'argent circule directement de l'acheteur au vendeur, sans transiter par un intermédiaire, mais ils sont relativement moins sécuritaires – surtout en ce qui concerne les dangers de la fraude par copiage. De plus, en éliminant les intermédiaires, ces systèmes impliquent des transactions moins coûteuses. Ainsi, les systèmes hors-ligne sont, à notre avis, indiqués pour les transactions à faible valeur, notamment pour les micropaiements.

En ce qui concerne la symétrie, il est évident que les systèmes symétriques sont moins coûteux, nécessitant les mêmes outils tant pour l'acheteur que pour le vendeur, et ne requièrent pas, dans la plupart du temps, d'investissements additionnels – en équipements matériels. Ceci est, toutefois, réalisé au coût d'une complexité accrue au niveau de l'implantation logicielle.

Tableau 2.3 – *Classification et analyse comparative*

Critères d'analyse / Systèmes	Sécurité	RM	Pérennité de la MR	Configuration du système	Niveau d'anonymat	Granularité de la RM	Débit de fonds	Délai d'encaissement	Mode d'échange des fonds	Convertibilité de la RM	Niveau de développement
I – SYSTÈMES SANS ADHÉSION											
1) Modèle «sans protection»											
a) cartes de crédit / chèques											
Interface CGI du Web [BWAR]	faible	num.	limitée	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
2) Modèle «avec protection» *(en général encryptage avec SSL)*											
a) cartes de crédit											
BuyWay	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	exp.
ClearCommerce	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
CommerceXpert	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
E-money.NET	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
Net.Commerce	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
NetVerify	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	n. d.
Payline	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
Payway	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	n. d.
Secure-Bank.Com	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
SecureOrder	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
SecurePay	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
SecureProcess	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	n. d.
SecureLink	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
SecureTrans	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
TouchLink	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
WebCash	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.

Tableau 2.3 – *Classification et analyse comparative (suite)*

Critères d'analyse / Systèmes	Sécurité	RM	Pérennité de la MR	Configuration du système	Niveau d'anonymat	Granularité de la RM	Débit de fonds	Délai d'encaissement	Mode d'échange des fonds	Convertibilité de la RM	Niveau de développement
b) chèques											
OnlineCheck	moyenne	num.	u. u.	asymétrique	bas	grossière	anticipé	moyen	en-ligne	limitée	com.
Quick-Checks	moyenne	num.	u. u.	asymétrique	bas	grossière	anticipé	moyen	en-ligne	limitée	com.
II – SYSTÈMES AVEC ADHÉSION											
1) Modèle «authentification»											
a) mots de passe / *cookies*											
Protocole HTTP du Web [AMZN]	faible	num.	limitée	asymétrique	bas	grossière	différé	long	en-ligne	limitée	com.
b) «dépôt légal»											
Safe Purchase	faible	mdp.	illimitée	symétrique	bas	grossière	différé	long	en-ligne	nulle	exp.
2) Modèle «débit-crédit»											
a) NIP / mots de passe											
FirstVirtual	moyenne	NIP	illimitée	asymétrique	bas	grossière	différé	long	en-ligne	nulle	com.
Internet Dollar	moyenne	NIP	limitée	asymétrique	moyen	grossière	anticipé	long	en-ligne	nulle	rech.
WebCharge	moyenne	NIP	limitée	asymétrique	bas	grossière	anticipé	long	en-ligne	nulle	exp.
b) chèques électroniques											
AIMP	t. forte	num.	u. u.	n. d.	haut	n. d.	anticipé	court	en-ligne	n. d.	rech.
BankNet	forte	num.	u. u.	asymétrique	bas	grossière	anticipé	moyen	en-ligne	nulle	exp.
CheckFree	faible	num.	u. u.	asymétrique	bas	moyenne	différé	long	en-ligne	nulle	com.
CyberCoin	t. forte	num.	u. u.	asymétrique	haut	moyenne	différé	long	en-ligne	nulle	com.
E-Check	forte	num.	u. u.	asymétrique	bas	grossière	anticipé	moyen	en-ligne	nulle	rech.
NetCheque	moyenne	num.	u. u.	symétrique	bas	moyenne	anticipé	moyen	hors-ligne	nulle	rech.

Tableau 2.3 – *Classification et analyse comparative (suite)*

Critères d'analyse / Systèmes	Sécurité	RM	Pérennité de la MR	Configuration du système	Niveau d'anonymat	Granularité de la RM	Débit de fonds	Délai d'encaissement	Mode d'échange des fonds	Convertibilité de la RM	Niveau de développement
b) chèques électroniques (suite)											
NetChex	moyenne	num.	u. u.	asymétrique	moyen	grossière	anticipé	long	en-ligne	nulle	rech.
NetFare	faible	num.	limitée	asymétrique	haut	moyenne	anticipé	long	en-ligne	nulle	rech.
Redi-Check	moyenne	num.	u. u.	asymétrique	moyen	grossière	anticipé	long	en-ligne	nulle	com.
SNPP	faible	num.	u. u.	asymétrique	bas	n. d	anticipé	court	en-ligne	nulle	rech.
Vishnu	forte	cert.	u. u.	n. d.	bas	n. d	anticipé	court	en-ligne	n. d.	rech.
c) facturation / cartes de crédit											
ACC	t. forte	num.	u. u.	n. d.	haut	grossière	différé	long	en-ligne	n. d.	rech.
BlueMoney Network Wallet	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
ClickShare	moyenne	num.	u. u.	asymétrique	bas	moyenne	différé	long	en-ligne	limitée	exp.
Cybank	forte	num.	u. u.	asymétrique	bas	moyenne	différé	long	en-ligne	limitée	com.
CyberCash	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	com.
eCHARGE	moyenne	mdp.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	exp.
EVend	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	limitée	exp.
InterCoin	faible	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
iKP	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	totale	rech.
Klebox	t. forte	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	limitée	com.
NeosphereTollBooth	n. d.	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	limitée	com.
NetBill	t. forte	num.	u. u.	asymétrique	moyen	moyenne	anticipé	moyen	en-ligne	nulle	exp.
Pay2See	n. d.	num.	u. u.	symétrique	n. d.	n. d.	différé	n. d.	en-ligne	totale	com.
Web900	moyenne	mdp.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.
ZipLock	moyenne	num.	u. u.	asymétrique	bas	grossière	différé	long	en-ligne	totale	com.

Tableau 2.3 – *Classification et analyse comparative (suite)*

Critères d'analyse / Systèmes	Sécurité	RM	Pérennité de la MR	Configuration du système	Niveau d'anonymat	Granularité de la RM	Débit de fonds	Délai d'encaissement	Mode d'échange des fonds	Convertibilité de la RM	Niveau de développement
c1) Le sous-groupe SET											
e-Comm	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
GlobeSet	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
IBM Payment Suite	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	com.
ITP Wallet	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
SecureWeb Payments	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
VeriFone	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
WebWallet	t. forte	num.	u. u.	asymétrique	moyen	grossière	différé	long	en-ligne	limitée	exp.
3) Modèle «comptant»											
a) pièces numériques / billets virtuels											
Brands	t. forte	b. v.	limitée	asymétrique	haut	moyenne	anticipé	moyen	hors-ligne	totale	rech.
Camenisch, Piveteau & Stadler	forte	b. v.	u. u.	asymétrique	haut	n. d.	anticipé	moyen	en-ligne	n. d.	rech.
Chan, Frankel & Tsiounis	moyenne	b. v.	n. d.	n. d.	haut	n. d.	anticipé	n. d.	hors-ligne	n. d.	rech.
eCash	t. forte	b. v.	limitée	symétrique	haut	moyenne	anticipé	moyen	en-ligne	nulle	com.
Ferguson	forte	b. v.	u. u.	symétrique	haut	raffinée	anticipé	moyen	hors-ligne	n. d.	rech.
FOLC	t. forte	b. v.	n. d.	n. d.	haut	n. d.	anticipé	n. d.	hors-ligne	n. d.	rech.
IVC / GlobeID	n. d.	b. v.	n. d.	asymétrique	n. d.	n. d.	n. d.	n. d.	en-ligne	n. d.	com.
Jakobsson & Yung	t. forte	b. v.	limitée	n. d.	moyen	n. d.	anticipé	n. d.	hors-ligne	n. d.	rech.
Lysyanskaya & Ramzan	forte	b. v.	n. d.	n. d.	haut	n. d.	n. d.	n. d.	en-ligne	n. d.	rech.
Magic Money	moyenne	b. v.	limitée	symétrique	moyen	raffinée	anticipé	moyen	hors-ligne	n. d.	rech.

Tableau 2.3 – *Classification et analyse comparative (suite)*

Critères d'analyse / Systèmes	Sécurité	RM	Pérennité de la MR	Configuration du système	Niveau d'anonymat	Granularité de la RM	Débit de fonds	Délai d'encaissement	Mode d'échange des fonds	Convertibilité de la RM	Niveau de développement
a) pièces numériques / billets virtuels (suite)											
Mondex	forte	cptr.	illimitée	symétrique	haut	moyenne	anticipé	court	hors-ligne	totale	exp.
NetCash	faible	b. v.	limitée	symétrique	moyen	moyenne	anticipé	moyen	hors-ligne	nulle	rech.
PayMe	t. forte	b. v.	limitée	symétrique	haut	moyenne	anticipé	court	hors-ligne	nulle	rech.
PC Pay	forte	count.	illimitée	asymétrique	n. d.	moyenne	anticipé	moyen	en-ligne	limitée	com.
a1) Le sous-groupe des micropaiements											
Belle Micro Payment System	moyenne	cert.	limitée	asymétrique	moyen	moyenne	anticipé	n. d.	en-ligne	nulle	exp.
MicroMint	faible	b. v.	limitée	asymétrique	faible	raffinée	anticipé	long	hors-ligne	nulle	rech.
MilliCent	moyenne	b. v.	u. u.	asymétrique	moyen	raffinée	anticipé	long	en-ligne	limitée	exp.
MiniPay	forte	cert.	u. u.	asymétrique	faible	moyenne	anticipé	long	hors-ligne	nulle	exp.
MPTP	moyenne	num.	u. u.	symétrique	faible	raffinée	différé	long	hors-ligne	limitée	rech.
NetCard	moyenne	b. v.	limitée	asymétrique	faible	raffinée	anticipé	moyen	en-ligne	n. d.	rech.
PayWord	moyenne	cert.	u. u.	n. d.	bas	raffinée	différé	long	hors-ligne	n. d.	rech.
SOX	t. forte	b. v.	illimitée	asymétrique	moyen	arbitraire	anticipé	court	en-ligne	limitée	exp.
SubScrip	faible	num.	limitée	asymétrique	haut	raffinée	anticipé	moyen	hors-ligne	n. d.	rech.
SVP	forte	b. v.	n. d.	asymétrique	bas	raffinée	anticipé	long	hors-ligne	n. d.	rech.

Légende:
b. v. = pièces ou billets virtuels
cert. = certificats
com. = commercial
cptr.= compteur
exp. = expérimental (bêta)
mdp. = mots de passe
n. d. = non-disponible
num. = numéros de série, encryptés / signés ou non
rech. = recherche (alpha)
t. forte = très forte
u. u. = usage unique

Le délai d'encaissement est un aspect qui touche de très près les commerçants, qui, pour la plupart, ont intérêt à toucher leur fonds le plus tôt possible. Les systèmes offrant un court délai d'encaissement, tels que les systèmes du groupe «comptant», seront ainsi plus avantagés de ce point de vue.

Le débit de fonds est un aspect qui pourrait diviser les consommateurs en fonction de leurs intérêts et préférences financières. Ainsi, les systèmes permettant un débit de fonds différé offrent aux acheteurs la possibilité «d'acheter maintenant et payer plus tard», avec les avantages et les désavantages rattachés à cette méthode transactionnelle. Il est évident que les clients auront besoin d'une carte ou d'une marge de crédit pour pouvoir se prévaloir de tels systèmes électroniques de paiement sur Internet, ce qui donne une très grande influence aux banques émettrices – surtout en ce qui concerne la création de masse monétaire à l'intérieur du système. En effet, en augmentant les limites de crédit des clients, les banques peuvent accroître le pouvoir d'achat des usagers – ce qui augmentera non seulement les profits potentiels, mais aussi les risques de non-paiements, qui eux pourront engendrer des pertes. Par contre, les systèmes requérant un débit anticipé de fonds exigent l'acquittement complet de la contre-valeur de la RM, mais ils ouvrent la porte aux transactions numériques à ceux qui n'ont pas d'instruments de crédit.

L'utilisation de ces instruments – des cartes de crédit, notamment – n'est pas uniforme à travers le monde, ni même à travers les pays de l'OCDE. Ainsi, en Amérique du Nord ou en France, leur usage est largement répandu, mais il est assez restreint dans les pays de l'Europe Centrale et de l'Est, même dans des économies très puissantes, telles que l'Allemagne. De plus, en utilisant les cartes de crédit, les usagers renoncent volontairement à tout anonymat, chaque transaction pouvant être retracée par toutes les entités transactionnelles; l'analyse des habitudes d'achat et la publicité ciblée sont seulement quelques applications utilisant les informations tirées à partir de ces traces. Un autre aspect négatif provient du manque de granularité de ces instruments de

paiement et du montant minimal des transactions – qui, habituellement, doivent dépasser 5 $. Enfin, les coûts des transactions ne sont pas négligeables, les acheteurs devant payer souvent de 15 à 50 cents par achat, tandis que les vendeurs doivent acquitter aux banques un pourcentage de chaque transaction – en général, de 2 à 4%.

Un éventuel système qui permettrait d'éviter ces désavantages, en n'employant pas de cartes de crédit, et qui capitaliserait sur les avantages des systèmes symétriques, offrant aussi un court délai d'encaissement, pourrait se démarquer nettement de la concurrence. De plus, en utilisant le modèle «comptant» et la technologie du sous-groupe des micropaiements, un tel système pourrait répondre aux plus récents besoins des usagers, en terme de consommation spécialisée dans l'ère nouvelle de l'économie numérique.

En ce qui concerne les différents types de commerces, de nos jours, il existe encore une nette distinction entre les transactions commerciales électroniques qui ont lieu entre deux ou plusieurs entreprises et le commerce électronique au détail, qui a lieu entre une entreprise et un consommateur. Le commerce électronique interentreprises sur Internet augmente très rapidement à mesure que ces organisations, souvent habituées aux transactions par EDI, deviennent de moins en moins réticentes à transmettre leurs données par voie électronique.

Nous avons remarqué par ailleurs le fait que dans la plupart des systèmes destinés aux transactions interentreprises, l'EDI reste présent chaque fois qu'il s'agit d'une solution complète de commerce électronique. Il s'agit là de la convergence de l'EDI vers l'Internet, pour former ce que l'on appelle déjà WebEDI – EDI ayant un nouveau support, basé sur le Web, en transmettant, par exemple, des messages EDI traditionnels sur le réseau Internet, par courrier électronique.

En ce qui concerne d'autres standards, **Internet Purshasing Roundtable** développe le standard OBI (*Open Buying on the Internet*), avec le support de plusieurs grandes compagnies, telles que **IBM**, **Microsoft** et **Oracle**. Ce standard transactionnel vise principalement à assurer l'interopérabilité entre les systèmes de commerce électronique interentreprises sur Internet. Il spécifie un nouveau standard basé sur EDI, servant à formater les commandes transactionnelles, sans toutefois utiliser les normes de transmission employées par EDI.

2.6 Conclusion

Nous venons de passer en revue les principaux systèmes de paiement électroniques disponibles actuellement pour effectuer des transactions numériques sur Internet, en faisant ressortir leurs caractéristiques internes et externes, leurs avantages et leurs inconvénients. Pour ce faire, nous avons introduit quelques notions générales ainsi que plusieurs critères d'analyse et d'évaluation et nous avons effectué une analyse comparative en profondeur des différents systèmes.

En étudiant les points forts et les points faibles de ces systèmes, nous avons fait ressortir les besoins que devraient rencontrer le nouveau système que nous avons développé dans le cadre de cette thèse et qui sera présenté en détail dans le chapitre suivant. Ce système nous permettra de généraliser certains notions que nous venons de voir et d'introduire plusieurs nouveaux concepts qui ne se trouvent dans aucun des systèmes existants. De cette façon, nous pourrons employer une approche systématique permettant de cibler correctement les caractéristiques internes et externes d'un futur système transactionnel.

CHAPITRE 3

LE TRANSFERT NUMÉRIQUE DE VALEURS

Dans le monde commercial et financier, un des sujets les plus actuels concerne la transition vers l'argent numérique. Banques, détaillants ou fournisseurs de services Internet sont tous en train d'évaluer ou d'implanter de nouvelles technologies utilisant des transactions électroniques sécurisées, des cartes intelligentes ou d'autres solutions profitables dédiées au commerce électronique. Leur succès ne dépendra pas seulement de la technologie; d'autres aspects importants, tels que les aspects légaux, économiques, législatifs ou sociaux devront aussi être résolus.

Dans ce contexte, une étude comparative, telle que celle présentée dans le chapitre précédent, permet de voir les atouts et les manques des différents concepts sur lesquels sont basés plusieurs systèmes de paiement électronique. Elle nous permet aussi d'imaginer les éléments qu'un nouveau système pourrait contenir, afin de lui permettre de répondre à des besoins encore plus généraux. Notons que cette recherche bibliographique a été constamment mise à jour. Lorsque nous avons commencé la première version préliminaire de l'analyse de besoins d'un nouveau système, en janvier 1996, il y avait à peine une dizaine de systèmes de paiement électronique sur Internet, toutes catégories confondues. Depuis, ce nombre a augmenté rapidement, tandis que les

caractéristiques des différents systèmes ont commencé à se cristalliser en plusieurs groupes distincts. C'est pour cette raison que l'analyse des besoins présentée dans ce chapitre est basée surtout sur l'étude des systèmes les plus représentatifs.

Comme nous avons constaté dans notre étude au chapitre précédent, plusieurs systèmes électroniques de paiement existent, apportant chacun leurs solutions, avec leurs avantages et leurs inconvénients. Étant donnés les compromis qui doivent être faits à tous les niveaux du design, il est évident qu'il est pratiquement impossible de réaliser un algorithme ou une implantation sans aucun désavantage. Le survol des systèmes de paiement électronique nous a permis de voir quelles sont leurs caractéristiques principales et de démontrer le besoin d'un nouveau système de transfert de valeurs. Nous avons vu quels sont leurs points forts, quels points doivent être améliorés dans le design d'un nouveau système et quels points faibles doivent être évités, tout en essayant d'apporter des solutions innovatrices.

Nous nous proposons de construire dans le cadre de cette thèse les bases d'un système qui capitalisera sur plusieurs points forts de certains systèmes existants et de minimiser, voire d'éliminer, certains de leurs inconvénients respectifs, tout en apportant des solutions originales à plusieurs niveaux du design. Pour ce faire, nous allons introduire dans la section suivante un nouveau concept transactionnel qui vise à généraliser plusieurs notions que nous avons vues précédemment.

3.1 Analyse des besoins

La revue des systèmes effectuée dans le chapitre précédent nous montre que les solutions transactionnelles existantes ne peuvent accomplir qu'une seule tâche:

effectuer des paiements. Cependant, plusieurs applications actuelles, telles que la publication de documents électroniques ou les échanges bancaires, requièrent plus d'options et de fonctionnalités. Le transfert de fonds est un premier pas essentiel dans la bonne direction car, après tout, un billet virtuel n'est qu'un document numérisable, signé et certifié par une banque, mais il est facile de prévoir que cette approche ne sera pas suffisante dans les années à venir.

Dans ce contexte, nous avons décidé de réaliser un système plus général d'échange, permettant le transfert de toute représentation numérique ayant une valeur non-intrinsèque vérifiable. Pour ce faire, nous introduisons un nouveau concept, celui du «***transport, transfert et échange générique de valeurs***». Nous voulons ainsi réaliser un nouveau système, basé sur ce concept inédit, permettant l'échange commercial de l'argent numérique et des autres documents électroniques par l'intermédiaire d'un ***protocole unifié*** dédié aux transactions numériques. Ainsi, l'argent virtuel en particulier et le paiement électronique en général ne représente qu'une, parmi plusieurs «valeurs» transmissibles à l'aide de ce nouveau système.

3.1.1 Transport, transfert et échange de valeurs

Dans le cadre de cet ouvrage, nous définissons le terme ***transport*** comme étant le processus de transmission d'un document électronique – ou toute autre donnée numérique – d'un point A à un point B, soit en le copiant, mais surtout en le déplaçant, sans toutefois changer ou perdre les droits de propriété sur ledit document. De cette façon, le document est déplacé à un nouvel endroit, mais il continue d'appartenir au même propriétaire, qui continue d'avoir les mêmes droits sur le document qu'avant son transport.

Le terme ***transfert*** implique, en plus du transport du document, un changement de droits de propriété. Ainsi, lors d'un transfert, le propriétaire P cède tous ses droits sur le document transporté de l'endroit A_P à l'endroit B_R au nouveau propriétaire R. Notons que le transfert de propriété et la cession des droits se fait une fois que le document est arrivé à sa destination.

Enfin, l'***échange*** implique au moins deux transferts; d'un commun accord, en échange du document D_1 appartenant à son propriétaire P, le propriétaire R lui transfère le document D_2. Suite à ces deux transferts – donc à l'échange –, P cède tous ses droits sur D_1 et devient le nouveau propriétaire de D_2, tandis que R cède tous ses droits sur D_2 et devient le nouveau propriétaire de D_1.

3.1.2 Le paiement comme valeur transférée

Le concept de valeur ne signifie pas simplement des nombres bruts; l'histoire nous a montré qu'une façon intuitive de représenter la valeur, dans son sens économique le plus profond, était d'utiliser la valeur intrinsèque d'un bien. Depuis, le monde à beaucoup évolué, en passant par les pièces métalliques et les billets en papier, pour arriver au plastique et maintenant aux bits d'information, invisibles, mais néanmoins précieux.

Le terme ***valeur*** est un terme relatif. L'argent est peut-être l'exemple le plus connu de valeur concrète, mais ce n'est sûrement pas le seul. Tout objet peut représenter une certaine valeur pour son propriétaire. Dans cet ouvrage, nous allons utiliser ce terme pour faire référence à la représentation binaire de tout objet numérisable ayant une valeur quelconque pour son propriétaire. Ainsi, cette représentation binaire aura une valeur non-intrinsèque équivalente à la valeur de l'objet concret. La valeur peut aussi être une valeur ajoutée; ainsi dans le cas d'une communication, par exemple, le message

lui-même devient une valeur lorsqu'il est protégé par encryptage. Si son auteur (ou propriétaire) décide de le protéger, ceci implique qu'il représente une certaine valeur.

Des pièces ou des coupons électroniques, des billets virtuels, des certificats numériques ou d'autres informations se trouvant dans des documents numériques, prenant la forme de fichiers binaires, peuvent représenter des valeurs. Ainsi, des documents électroniques peuvent contenir des messages informationnels, mais aussi un ou plusieurs éléments parmi ceux qui nous venons d'énumérer.

3.2 Proposition d'un nouveau système

3.2.1 Concept général

En se basant sur nos analyses [Ureche et Plamondon, 1996], [Ureche et Plamondon, 1998a], [Ureche et Plamondon, 1998b], nous introduisons un nouveau système transactionnel, permettant le transport de valeurs numériques sur des réseaux numériques de communication, sans restriction quant à leur nature intrinsèque. Le nouveau système permettra le transport, le transfert et l'échange généralisé de valeurs, basé sur le concept d'***enveloppes virtuelles***. De cette façon, l'argent virtuel devient une valeur parmi une foule d'autres valeurs transportables sur des réseaux de communications électroniques. Un avantage immédiat du système: les enveloppes virtuelles permettent de prendre comme charge tout autre objet numérique, tels que les certificats, les coupons, les factures ou les pièces d'identité.

Ce nouveau système, nommé TRANZIX, vise à offrir les bases d'un nouvel outil de paiement et d'échange de documents électroniques, rendant possibles les

transactions numériques généralisées sur des réseaux de communications non-sécuritaires. De cette façon, les transactions électroniques deviennent substantiellement plus flexibles, le nouveau système permettant leur transport, leur transfert et leur échange, en utilisant un même support, un même protocole et un même logiciel. Par exemple, un transfert de fonds peut être accompagné par d'autres documents informationnels signés et certifiés numériquement; ainsi, le transfert générique de valeur est réalisé sans une augmentation significative des coûts ou de la puissance de calcul reliée à la transaction. Nous parlons donc – comme le titre de l'ouvrage le suggère – d'un système électronique qui permet d'effectuer des transactions commerciales – qui consistent généralement en un transfert de valeur – de façon numérique, et ceci, sur des réseaux de communication informatiques.

En même temps, le système intègre l'aspect microtransactionnel, permettant ainsi d'augmenter la granularité d'une devise. À cet égard, le système est dimensionné pour faire face à un volume important de transactions avec un faible coût de traitement par transaction; pour des produits ou services à quelques cents l'unité, le système permettra de fonctionner efficacement avec des coûts marginaux de moins d'un cent par transaction.

Il est évident que tous les systèmes basés sur le modèle «débit-crédit» ou qui utilisent de façon directe ou indirecte des cartes de crédit ne sont pas utilisables dans un protocole qui se propose d'implanter des micropaiements, à cause du coût par transaction engendré par les chèques ou cartes de crédit bancaires. Ceci implique un choix fondamental: le système proposé ne sera pas basé sur le modèle «débit-crédit» et n'utilisera pas de façon directe des cartes de crédit, mais plutôt des billets virtuels prépayés, ayant une valeur monétaire dès leur émission. Afin d'éliminer ou au moins de limiter les inconvénients des protocoles étudiés et profiter de certains de leurs avantages, le nouveau système transactionnel devra faire face aux défis suivants:

- assurer un haut niveau de sécurité [Heintze et Tygar, 1996], d'authentification et de protection de la vie privée [Belotti, 1997], [Burkert, 1997]; même si en général les réseaux informatiques publics ou privés, particulièrement l'Internet, ne fournissent pas de tels avantages, le système proposé devra résoudre ce problème, garantissant ainsi un haut niveau de confiance dans cet environnement transactionnel;
- permettre une grande portabilité à un faible coût initial; pour avoir des chances d'être accepté commercialement, le système devra pouvoir être implanté sur plusieurs plates-formes et de préférence sans coûts initiaux additionnels pour des modules matériels dispendieux;
- assurer la gestion et l'administration locale des transactions et des comptes; les usagers du système, clients et vendeurs, doivent être capables de faire le suivi du flux de leur argent et de leurs transactions;
- faire un compromis entre les systèmes en-ligne et hors-ligne, afin de tirer avantage de leurs points forts, tout en minimisant ou éliminant leurs points faibles; ceci pourra se réaliser en donnant à l'usager la possibilité de choisir le mode de transfert en fonction de l'importance des transactions. Le système ainsi conçu présentera une flexibilité unique qui permettra de répondre sur mesure aux besoins des usagers;
- ne pas distinguer, de façon générale – ou minimiser toute distinction – entre l'entité transactionnelle acheteur et l'entité transactionnelle vendeur. Le résultat sera un système symétrique extrêmement portable d'une plate-forme à une autre, où deux usagers pourront transiger sans que l'un de deux ne dispose d'un équipement (logiciel ou matériel) spécial;
- conférer une grande portabilité aux billets virtuels; à l'aide des transactions numériques généralisées basées sur le concept d'enveloppes virtuelles, permettre des «échanges mixtes» de valeur, contenant par exemple de documents électroniques accompagnés de billets virtuels, certificats et signatures numériques, etc.

3.2.2 Choix de design

Pour assurer un haut niveau potentiel de pénétration au niveau commercial et faciliter son installation et son utilisation, le système proposé sera donc symétrique et exclusivement logiciel; donc ni l'acheteur ni le vendeur n'auront à acheter des équipements dédiés et de plus, chacun pourra utiliser le même logiciel tant pour vendre que pour acheter. Pour renforcer la grande flexibilité proposée du système, une grande variété de valeurs pourra être échangée – rendant ainsi nécessaire l'adhésion des utilisateurs au système afin d'assurer une très forte sécurité.

Nous nous proposons de réaliser un système mixte, ou ***bimodal***, qui laisse à l'usager le choix d'effectuer une transaction en-ligne – donc plus sécuritaire, pour les transferts importants – ou hors-ligne – plus rapide, pour les transferts à faible valeur, comme les micropaiements. Dans ce dernier cas, le système sera direct; il n'utilisera pas d'intermédiaires lors du transfert de valeurs.

Étant donné que pour chaque transaction un client doit se connecter au vendeur ou à la banque, de façon rapide, efficace et sécuritaire, le choix réaliste de protocole de transmission sera le protocole TCP [Référence électronique RFCD]. Le protocole UDP [Référence électronique RFCD], même s'il est souvent plus rapide et engendre moins de bits supplémentaires de transmission (*overheads*), ne garantit pas l'arrivée des datagrammes[1] à destination, ce qui est inacceptable, surtout dans un environnement qui se veut très sécuritaire. Comme les plates-formes serveurs, utilisant des systèmes d'exploitation dérivés de Unix [Hein et al., 1995], sont parmi les plus répandues dans le monde des communications numériques, ce système d'exploitation sera la plate-forme de choix dans le cadre du présent projet – surtout en ce qui concerne l'entité banque, entité qui devra faire être capable de face à une importante quantité de trafic. Toutefois, les ordinateurs personnels employant d'autres systèmes d'exploitation,

[1] Paquets d'information utilisés par le protocole UDP.

tels que Windows ou MacOS, détiennent une partie très importante du marché des systèmes client et ne peuvent donc pas être ignorés. Il serait donc intéressant d'essayer de garder une compatibilité avec ces plates-formes afin de permettre une bonne portabilité du système – surtout pour l'entité client.

3.2.3 Sécurité et personnalisation

Étant donné l'excellent rapport qualité-prix offert par les moyens cryptographiques de sécurisation, nous allons utiliser un ou plusieurs mécanismes d'encryptage pour assurer la confidentialité et le contrôle d'accès dans notre système. Nous allons utiliser des signatures numériques afin d'assurer l'intégrité et l'authenticité des transactions. À la base de ces transactions numériques, nous allons utiliser des enveloppes virtuelles prenant la forme de billets numériques multi-fonctionnels, personnalisés à l'aide des technologies biométriques, en utilisant par exemple les signatures manuscrites des utilisateurs; ces technologies seront employées comme partie intégrante du processus d'encryptage. De cette façon, le système permettra d'assurer un haut niveau de sécurité, protégeant ainsi et les banques émettrices et leurs clients. Ceci permettra d'un coté de décourager toute tentative de contrefaçon et de l'autre, d'avoir l'assurance que toute fraude pourra être liée à son auteur. De plus, le système devra assurer un compromis raisonnable entre le besoin de confidentialité des consommateurs et le besoin des gouvernements de lutter contre le crime organisé – notamment le blanchiment d'argent.

Notons ici le fait que nous utilisons le terme signature en trois circonstances différentes. Ainsi, une ***signature manuscrite*** est le tracé que le client produit sur le formulaire de demande d'ouverture de compte à la banque, lors de l'adhésion au système. La ***signature numérisée*** est constituée par l'image binaire de la signature manuscrite, image obtenue à l'aide d'un numériseur. Finalement, une ***signature***

électronique ou ***numérique*** est une suite de nombres binaires obtenue à l'aide d'une clé secrète, en employant un algorithme cryptographique asymétrique.

L'acquisition des signatures manuscrites des utilisateurs se fera, comme nous l'avons mentionné, lors de l'adhésion, en numérisant le formulaire d'ouverture de compte. Ainsi, l'équipement matériel ne sera utilisé ni par l'entité client, ni par l'entité vendeur, mais seulement par la banque, pour laquelle les coûts d'installation seront minimaux.

3.3 Objectifs

Depuis le début de cette thèse, nous nous sommes fixé quelques objectifs clairs et concrets, visant à bien nous guider pendant la réalisation du projet. Même si quelques-uns de ces objectifs ont subi certaines modifications en cours de route, le mandat initial reste identique. Un apport tout particulier à ce niveau a été amené par l'examen de synthèse qui nous a permis de mieux définir le cadre, les objectifs et l'étendue du travail à réaliser.

Le mandat de base de notre travail est donc de poser les fondations théoriques d'une possible économie microtransactionnelle numérique. Pour ce faire, nous avons fixé comme premier objectif l'introduction d'une nouvelle taxonomie accompagnée d'une liste de critères d'analyse permettant de réaliser une toute première revue quasi exhaustive des systèmes électroniques de paiement sur Internet. Nous avons présenté dans le chapitre précédent les résultats de ce travail intégrateur de synthèse. Dans un deuxième temps, nous nous proposons d'effectuer la description détaillée des concepts généralisant la notion de paiement comme valeur transigée et comme opération

transactionnelle que nous avons brièvement introduits dans ce chapitre. Troisièmement, nous allons réaliser les spécifications fonctionnelles et le design préliminaire du système TRANZIX, le premier à utiliser une approche bimodale ayant des supports physiques multiples de communication. Un autre élément original sur lequel nous allons nous attarder réside au niveau de la sécurité qui sera assurée à l'aide des technologies de protection utilisant des mécanismes cryptographiques ainsi que des moyens biométriques d'identification. Quatrièmement, nous allons démontrer la faisabilité des concepts et des notions introduites en construisant un premier prototype expérimental et nous allons analyser et interpréter les résultats obtenus. Enfin, nous allons regarder les impacts possibles de tels systèmes au niveau économique et social, nous allons nous interroger sur les divers scénarios possibles d'implantation commerciale et nous allons discuter différentes solutions de déploiement à grande échelle.

3.4 Conclusion

À l'aide des conclusions tirées du travail de recherche bibliographique, les exigences d'un nouveau système électronique de transfert de valeurs ont été énumérées. Nous avons aussi introduit dans ce chapitre plusieurs définitions de base sur lesquelles ce nouveau système reposera, définitions qui généralisent certaines notions présentées dans le chapitre précédent. Nous avons ainsi défini le paiement comme valeur transférée, ainsi que le transport, le transfert et l'échange de valeurs. Par la suite, les grandes lignes du nouveau système transactionnel ont été élaborées, en exposant son concept général. Quelques choix de design ont été effectués avant de présenter brièvement plusieurs aspects concernant les moyens de sécurité et de personnalisation du système.

CHAPITRE 4

LE SYSTÈME TRANZIX

Nous allons présenter en détail dans ce chapitre un nouveau système transactionnel, outil unique de transport, de transfert et d'échange numérique de valeurs, système que nous avons appelé TRANZIX. Nous allons débuter avec la présentation générale du concept de base, des spécifications fonctionnelles des entités du système, de l'environnement de travail et du diagramme de flux de données (DFD). Nous allons nous pencher par la suite sur le design préliminaire du nouveau système, en présentant son diagramme hiérarchique (DH), la description des interfaces et les différentes structures de données.

Afin d'assurer un haut niveau de confiance dans ce nouveau système, nous allons expliquer le traitement des exceptions, qu'il s'agisse d'erreurs de fonctionnement, de pannes ou de fraudes internes ou externes au système. Enfin, une explication détaillée des méthodes de protection de TRANZIX sera exposée, en introduisant les mécanismes de sécurisation cryptographiques ainsi que les moyens de personnalisation biométriques que nous avons employé. Une brève discussion sur les autres alternatives de protection sera aussi incluse.

4.1 Le concept de base

Comme nous avons montré dans les sections précédentes, la plupart des systèmes transactionnels existants sont des systèmes exclusivement financiers, en ce sens qu'ils servent seulement d'outils pour effectuer des paiements électroniques. Suite à l'analyse des besoins présentée dans le chapitre précédent, nous avons déterminé une liste d'exigences à rencontrer par un nouveau système transactionnel, hautement flexible, basé sur le concept générique de «transfert généralisé de valeurs». Ainsi, un des aspects les plus importants de ce concept est constitué par la capacité intrinsèque du nouveau système de transporter des valeurs, sans restriction quant à ce qu'elles représentent – donc tout document numérique valant quelque chose pour quelqu'un.

Ce nouveau système électronique permet d'effectuer le transport, le transfert et l'échange de valeurs et comporte les quatre entités transactionnelles, définies dans la sous-section 2.3.1. Notons que dans notre système, au niveau technique du design, ces quatre entités sont regroupées en deux ensembles; ainsi, le premier ensemble contient l'entité acheteur et l'entité vendeur et sera appelé «la partie client» (ou l'«entité client»), puisque TRANZIX est un système symétrique, dans lequel les deux entités peuvent s'échanger librement les rôles. Le deuxième ensemble sera appelé «la partie banque» (ou l'«entité banque»), car, généralement, la banque jouera en même temps le rôle d'émetteur.

Nous avons établi au Chapitre 3 le fait que le système TRANZIX utilise le concept d'enveloppes virtuelles comme moyen de transport généralisé de valeurs et celui de billets numériques comme moyen de transfert financier – les messages échangés lors d'une transaction pourront avoir une valeur marchande, étant payés d'avance. Ceci implique l'utilisation de technologies d'encryptage fort afin d'assurer non seulement la confidentialité des transactions, mais aussi leur sécurité, tant pour la banque émettrice –

celle qui a émis ces billets en échange de l'argent réel –, que pour les clients, qu'ils soient vendeurs ou acheteurs. De plus, TRANZIX assure un compromis raisonnable entre le besoin de confidentialité des consommateurs et le besoin des gouvernements de lutter contre le crime organisé – notamment le blanchiment d'argent.

Le système est direct, donc sans intermédiaires, symétrique et exclusivement logiciel, tant pour les acheteurs que pour les vendeurs. Seule la banque émettrice utilisera un module matériel ayant la forme d'un numériseur d'image (scanner). Ce que le système proposé apporte au niveau de l'originalité c'est la très grande flexibilité qu'il offre aux usagers. Ainsi, à ce jour, c'est le premier ***système intégré mixte***, offrant non seulement le choix des documents numériques à transporter, transférer ou échanger, mais aussi la façon par laquelle ces opérations peuvent être effectuées; les utilisateurs pourront donc choisir entre les transactions en-ligne et hors-ligne, ainsi que le choix de la modalité de communication entre les entités transactionnelles. Nous offrons ainsi à l'usager la possibilité de choisir le mode de transfert en fonction de l'importance des transactions.

TRANZIX implante aussi le concept de micropaiements, raffinant ainsi la granularité de la devise utilisée comme moyen de couvrir les transferts – le dollar canadien en ce moment. Le système ainsi conçu présente une flexibilité unique qui permet de répondre sur mesure aux besoins des usagers. L'utilisation d'une telle approche permet l'intégration du logiciel dans une plate-forme Web ou dans une architecture intranet, permettant d'effectuer des transactions – financières ou non – entre les différents départements administratifs d'une entreprise. Un premier aperçu du flux des données transactionnelles à l'intérieur du système est montré dans la Figure 4.1 [Ureche et Plamondon, 1999c].

Un autre aspect original de TRANZIX réside à l'intérieur même de la structure des messages transactionnels. Pour assurer la protection des valeurs véhiculées

par le système, nous utiliserons des méthodes cryptographiques, ainsi qu'une ***mémoire active*** – ou historique – pour chaque billet virtuel. Ainsi, l'authentification des messages transactionnels comportera une ***identification biométrique*** de chaque client, afin d'assurer un haut niveau de sécurité au système.

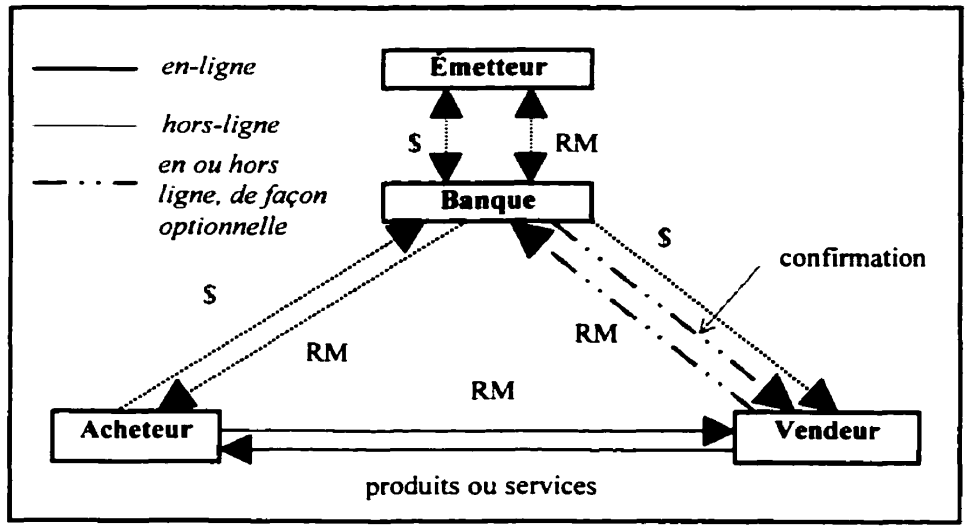

Figure 4.1 – *Le flux des données transactionnelles dans le système TRANZIX*

Une des méthodes les moins coûteuses pour effectuer des identifications biométriques, tout en restant efficace, est l'utilisation de la signature manuscrite des clients, signatures présentes dans les formulaires d'ouverture de compte. À partir de ces signatures manuscrites et d'un algorithme cryptographique permettant d'effectuer des signatures numériques, nous allons créer une ***signature biométrique*** permettant d'identifier une personne par ses signatures manuscrites et électroniques. L'identification biométrique représentée par cette signature biométrique est désignée par le terme ***ID-biométrique***. Ainsi, le système protège tant les banques que les usagers, ce qui permettra d'un côté de décourager toute tentative de contrefaçon et de l'autre, d'avoir l'assurance que toute fraude pourra être liée à son auteur. Cet aspect sera développé en détail à la section 4.4.

4.2 Spécifications fonctionnelles

Dans cette section nous allons effectuer la description du système TRANZIX, en insistant sur les moyens que nous envisageons d'implanter pour satisfaire aux besoins des usagers – tels que décrits dans l'analyse des besoins – et pour réaliser l'interface entre le système et son environnement. Nous allons aussi présenter le diagramme de flux de données, représentation graphique permettant de décrire la propagation des données et les différentes transformations qu'elles subissent dans le système.

Le nouveau système électronique de transport, transfert et d'échange numérique de valeurs est basé sur un nouveau protocole que nous introduisons dans cet ouvrage, le ***protocole de transfert d'enveloppes virtuelles*** (PTEV) sur les réseaux numériques de communication. Avant d'être envoyée sur le réseau, la charge transférée prend une forme standardisée, propre aux enveloppes virtuelles. Les documents électroniques qui seront échangés peuvent être obtenus à l'aide de la banque – ou en général, d'un émetteur ou d'une autre autorité de certification. De cette manière, les documents sont non seulement rendus dans le format standardisé exigé par le PTEV, mais ils sont aussi certifiés et signés par l'autorité de certification – généralement la banque.

TRANZIX permet donc à toutes les entités d'utiliser le même portefeuille virtuel pour transporter, transférer ou échanger tout objet numérisable ayant une valeur non-intrinsèque, incluant des documents électroniques, des certificats, des pièces, des coupons et, en particulier, de l'argent. Utilisant le PTEV, n'importe quelle valeur peut être transportée, transférée ou échangée électroniquement, d'une façon rapide, transparente, conviviale et ergonomique. L'utilisation des billets numériques pour compléter la charge transmise peut ainsi constituer un cas typique d'utilisation du

système. Comme cette solution n'implique pas des équipements matériels coûteux, TRANZIX offre de très bas coûts d'installation et de maintenance. Le portefeuille logiciel peut ainsi servir comme classeur pour les documents électroniques des clients, complété d'un porte-monnaie numérique pour l'argent virtuel.

Le client peut lui-même être un certificateur, dans la mesure où sa signature est acceptée par les homologues transactionnels qui lui font confiance; il pourra ainsi certifier et émettre ses propres documents électroniques. En ce qui concerne les transactions financières, les billets virtuels peuvent être achetés généralement auprès d'une banque – ou d'un autre émetteur – avec tout instrument financier du «monde réel» tels que l'argent liquide, des chèques, des mandats postaux, des cartes de débit ou de crédit, etc. De cette manière, à l'aide de son protocole unifié, TRANZIX permet d'effectuer des ***transferts mixtes de valeur***, généralisant ainsi la notion de paiement électronique sur Internet. L'image générale du protocole étendu et du flux des données transactionnelles est présentée dans la Figure 4.2, dans laquelle l'échange d'argent est complété par l'échange d'autres documents numériques.

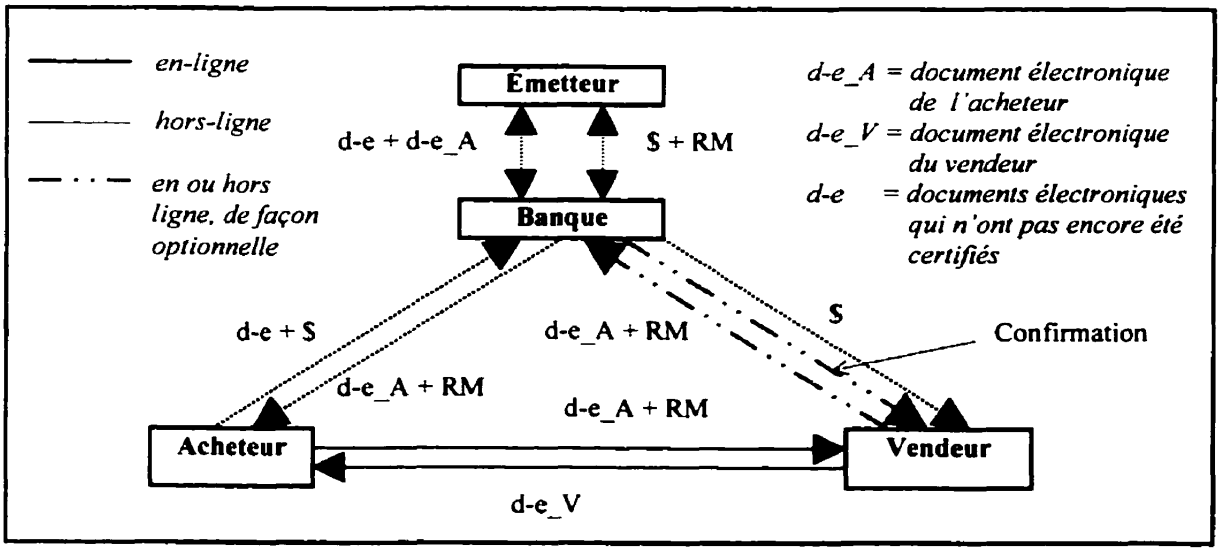

Figure 4.2 – *L'échange généralisé de valeurs*

Le système comprend deux logiciels séparés: un premier logiciel sert l'entité client, tandis que l'autre servira l'entité banque. Seule l'entité banque utilisera des équipements matériels, notamment des équipements capables de numériser des signatures manuscrites qui se trouvent sur des supports en papier. Du point de vue de la communication, les deux parties remplissent aussi bien les fonctions de serveur que les fonctions de client, puisque chaque entité doit être capable d'initier des transactions et de répondre à d'éventuelles requêtes transactionnelles. Ceci implique que les mêmes modules de communication – à quelques détails près – seront utilisés tant par l'acheteur et le vendeur que par la banque.

Nous employons le terme ***centres de traitement*** pour désigner un ou plusieurs modules spécifiques du logiciel de chacune des deux parties, conçus pour réaliser des tâches particulières. Une liste des fonctions qui sont effectuées par les deux parties sera présentée dans les paragraphes qui suivent.

4.2.1 Spécifications de l'entité client

Le système de transfert numérique généralisé de valeurs TRANZIX est destiné à faire face à un usage intensif. Il est donc essentiel qu'il soit facile à installer, à comprendre et à utiliser de façon répétitive. Ainsi, le logiciel permettra à l'entité client – terme qui inclut ici tant l'entité acheteur que l'entité vendeur, vu la symétrie du système – d'effectuer toutes les étapes d'une transaction de façon simple, rapide et transparente. L'usager pourra aussi entrer, à l'aide du clavier de son ordinateur, certaines données ou informations nécessaires au démarrage et au bon fonctionnement du système transactionnel. Le logiciel client comprend les fonctions suivantes:

1. Ouverture de compte;
2. Fermeture de compte;

3. Dépôt;
4. Retrait;
5. Transfert de documents numériques ou de billets (par exemple: d'un client à un autre, d'un compte à un autre dans la même banque, ou d'un compte à un autre dans des banques différentes mais qui utilisent le même système);
6. Paiement;
7. Facturation (lancer la requête d'un paiement ou d'un document);
8. Annulation d'un transfert (ou d'un paiement);
9. Échange de billets (expirés ou différentes coupures entre elles);
10. Informations sur le solde;
11. Fonctions locales:
    - consultation de la liste des transactions effectuées;
    - changement du mode de communication (en-ligne, hors-ligne ou par courrier électronique);
    - consultation du manuel d'utilisation interactif;
    - consultation du contenu du portefeuille virtuel.

Le logiciel peut être démarré automatiquement. Ainsi, pour un acheteur, le logiciel peut être activé au démarrage de son ordinateur ou juste avant d'effectuer une transaction. Pour le vendeur, le logiciel est activé par un ou plusieurs scripts qui servent, comme nous allons le voir en détail dans le chapitre suivant, d'interface entre le serveur Web de son cyber-magasin et son portefeuille virtuel.

4.2.2 Spécifications fonctionnelles de l'entité banque

La partie banque nécessite une attention toute particulière, étant donné le rôle vital qu'une banque émettrice joue dans le cadre d'un système économique. La

banque peut certifier des documents et émettre de l'argent, ce qui implique une attention spéciale quant à la création de la masse monétaire virtuelle. L'entité banque devra gérer, entre autres, les fonctions suivantes[1]:

1. Ouverture d'un compte;
2. Fermeture d'un compte;
3. Dépôt;
4. Retrait;
5. Transfert de documents numériques ou de billets
6. Paiement;
7. Facturation;
8. Annulation d'un transfert (ou d'un paiement);
9. Échange des billets;
10. Autorisation d'une transaction;
11. Informations sur le solde de chaque client;
12. Génération des billets et des certificats;
13. Gestion des adhésions
    - Collecte des données d'identification (formulaire d'ouverture de compte, signature manuscrite);
    - Stockage des données d'identification;
    - Génération des signatures électroniques et biométriques;
14. Gestion des clés;
15. Gestion des comptes;
16. Stockage des numéros de série des billets déjà déposés;

[1] Notons que plusieurs fonctions parmi celles mentionnées ici sont des fonctions essentielles au travail adéquat de toute institution financière, mais, étant donnée leur complexité – qui dépasse largement le cadre de notre mandat – elles ne sont mentionnées ici que pour offrir des spécifications fonctionnelles complètes.

17. Vérification des billets et des autres documents électroniques certifiés – comparer et détecter un numéro de série avec la liste des numéros des billets déjà déposés;
18. Détection et poursuite des éventuels fraudeurs;
19. L'acquittement et le clearing interbancaire.

La signature de la banque est une signature électronique générée à l'aide du protocole de génération de signatures d'un algorithme cryptographique à clés asymétriques. Par ailleurs, la signature de l'usager comprend, en plus d'une signature électronique – tel que déjà mentionné brièvement –, des moyens physiques d'identification. Nous allons voir en détail dans la section 4.4 portant sur les moyens employés pour assurer la protection du système TRANZIX comment utiliser un patron (*pattern*) numérique de la signature manuscrite d'un usager pour renforcer la sécurité assurée par notre système.

4.2.3 L'environnement de travail

Nous poursuivons l'étude des spécifications fonctionnelles par une analyse conduisant au choix d'un système d'exploitation et d'un langage de programmation. Nous apportons aussi quelques précisions sur la documentation du système. Il s'agit ici d'une étape clé dans la poursuite systématique de tout projet d'envergure.

4.2.3.1 Choix d'un système d'exploitation

Comme nous l'avons montré à l'étape précédente du projet, étape portant sur l'analyse des besoins, le système est basé intrinsèquement sur la communication entre les différentes entités. Ces entités peuvent se trouver sur des plates-formes différentes, par conséquent un protocole standardisé de communication doit être adopté;

la meilleure façon de communiquer à l'heure actuelle dans un tel environnement hétérogène est l'utilisation du protocole de communication électronique TCP. Le protocole TCP est utilisé dans notre système de préférence au protocole UDP, parce qu'entre autres ce dernier ne garantit pas l'arrivée des datagrammes à leur destination; par contre, TCP/IP forme un «circuit virtuel» en établissant une ligne virtuelle directe entre deux entités communiquantes.

Le système d'exploitation préféré pour l'utilisation de TRANZIX sera compatible avec le système d'exploitation sur lequel le protocole TCP/IP a été conçu – et pour lequel il a été initialement destiné, notamment les systèmes UNIX. Concrètement, nous allons utiliser le système d'exploitation Linux. Cependant, pour assurer un succès commercial raisonnable, il faudrait avoir un niveau élevé de compatibilité avec les autres systèmes d'exploitation, utilisés par une majorité d'utilisateurs d'ordinateurs. Ceci pourrait être réalisé, d'un coté en se basant sur un code modulaire et portable, et d'un autre, en compilant le code ainsi obtenu sur chacun de ces systèmes d'exploitation ou en utilisant un langage multi-systèmes comme Java.

4.2.3.2 Choix d'un langage de programmation

Le choix d'un langage de programmation est grandement simplifié par le choix du système d'exploitation, du protocole de communication et par la nécessité d'assurer à TRANZIX une grande portabilité. Un langage qui se prête bien à un environnement multi-plates-formes est le langage multi-systèmes Java. Notons toutefois, le fait que certains modules d'interface ou utilitaires d'aide, surtout ceux qui viseront à faciliter l'intégration du système au Web, pourront être écrits en utilisant d'autres langages de programmation, tels que HTML, ShellScript ou Perl.

4.2.3.3 Documentation

La documentation est une partie essentielle d'un produit commercial à succès. La documentation doit couvrir tous les aspects importants du système, pour toutes les entités impliquées. Elle doit porter sur les modalités d'installation, d'utilisation et de maintenance des logiciels qui forment le système. Elle doit s'adresser aussi bien au spécialiste qu'à l'utilisateur qui découvre pour la première fois ce nouvel environnement transactionnel. La disponibilité en plusieurs langues sera un excellent atout commercial.

Comme notre système transactionnel n'est pas rendu à une phase de développement commercial nécessitant une implantation à large échelle, ces exigences ne seront pas nécessaires en ce moment. La documentation comprendra plutôt cet ouvrage, qui pourrait être accompagné par d'autres documents connexes, électroniques ou non, qui sont suffisamment pertinents.

4.2.4 Le diagramme de flux de données

Nous allons définir dans cette sous-section la façon par laquelle les données circulent à l'intérieur du système électronique de transfert numérique de valeurs, en construisant le diagramme de flux de données, à plusieurs niveaux d'abstraction. Nous allons montrer les entrées/sorties (E/S), ainsi que les différents modules et centres de traitement des informations du système. Le flux des données est clairement marqué à chaque niveau d'abstraction. Pour faciliter la compréhension, nous avons décidé de présenter séparément l'entité client (Fig. 4.3) et l'entité banque (Fig. 4.6).

Concrètement, nous allons décrire deux niveaux de raffinement. Le premier niveau présente chaque entité de façon globale, avec ses grandes lignes directrices. Le

deuxième niveau explicite chacun des principaux centres de traitement en décrivant leurs principaux sous-modules et la façon à laquelle les données transactionnelles sont traitées.

Tous les modules et les sous-modules, qu'ils soient logiciels, matériels ou mixtes sont numérotés. Cette numérotation est effectuée de la manière suivante: tout d'abord, une lettre indique l'entité («c» pour l'entité client et «b» pour l'entité banque); ensuite, un premier nombre indique le niveau de raffinement et un deuxième indique le numéro du module.

Dans le raffinement de chaque centre de traitement, le premier nombre indique toujours le niveau de raffinement, le deuxième nombre indique le numéro du module qui a été explosé et un troisième indique le numéro du sous-module qui entre dans la composition du module respectif. Par exemple, c-2.9.5 indique le sous-module appelé «Payer», appartenant à l'entité client, qui se trouve au deuxième niveau de raffinement et qui est le cinquième sous-module faisant partie du module «Gérer les transactions (client)» (c-2.9).

4.2.4.1 L'entité client

L'entité client (Fig. 4.3) comporte une dizaine de modules, dont deux représentent des centres de traitement. Trois types d'entrées son prévues: l'interface entre l'utilisateur et le système, par laquelle l'usager peut entrer des commandes, des instructions et d'autres données, à l'aide d'un clavier, par exemple; le réseau numérique de communication et, optionnellement, un support physique de stockage, servant tous les deux d'entrées des messages transactionnels, qu'ils soient des billets virtuels ou des documents numériques.

L'acquisition des données est effectuée par trois modules spécialisés, c-1.4 «Lire les données d'interface», c-1.5 «Acquérir les transactions» et c-1.6 «Lire le support de stockage». Le réseau numérique de communication et, éventuellement, un support physique de stockage représentent deux des trois sorties du système. Notons qu'elles ont les mêmes numéros car, après avoir traité les données transactionnelles, TRANZIX emploie le même support de communication et de stockage pour conclure une transaction. L'écran est le troisième module matériel utilisé comme sortie du système, il offre au client des rétroactions visuelles.

À l'intérieur de l'entité client, le traitement des données est effectué par plusieurs modules, selon le type de donnée à traiter. Ainsi, les messages transactionnels sont tout d'abord traitées par le module c-1.8 «Vérifier localement l'intégrité des données» qui examine leur intégrité physique et logique. Les commandes de l'usager sont traitées par le module c-1.7 «Interpréter commandes du client» qui va les transformer en requêtes internes ou externes.

Une fois validées, les transactions sont exécutées par le centre de traitement des transactions c-1.9. Les réponses requises par le protocole transactionnel sont gérées suivant le type de destinataire; ainsi, les transactions avec un autre client – qu'il s'agisse de transferts de documents électroniques, de ventes numériques, etc. – sont gérées par le module c.1.11 «Commander les actions transactionnelles». Ce module sert, par exemple, à préparer un document numérique pour son transfert, vérifie les conditions d'un éventuel échange ou permet d'interagir avec un serveur Web d'un magasin virtuel, dans le cas d'une vente électronique. Les transactions avec la banque sont gérées par le module c-1.10 «Gérer les opérations bancaires».

Les deux centres de traitement de l'entité client sont explicités au deuxième niveau de raffinement. Ainsi, la Figure 4.4 permet de voir en détail le centre de traitement «Gérer les transactions (client)». Ce centre représente le «cœur

transactionnel» du logiciel, groupant une dizaine de sous-modules spécialisés dans les transactions financières.

Deux types d'opérations sont réalisés: les transactions courantes, ou répétitives, – telles que payer, retirer, déposer – et les transactions singulières – telles que l'ouverture ou la fermeture d'un compte. Notons que pour les transactions non-financières – le transfert de documents certifiés ou d'autres objets virtuels –, le sous-module c-2.9.6 «Transférer» est utilisé dans une direction de transfert – pour les transferts vers l'extérieur du portefeuille virtuel local – et le sous-module c-2.9.4 «Facturer» est employé dans l'autre direction de transfert – pour les transferts vers l'intérieur du portefeuille virtuel.

La Figure 4.5 montre en détail le centre de traitement «Gérer les communications (client)». C'est ici que les données sont assemblées, encryptées et emballées dans les enveloppes virtuelles. D'autres opérations sont aussi prises en charges par les autres sous-modules appartenant à ce centre de traitement, par exemple la gestion du mode de communication ou des clés d'encryptage.

4.2.4.2 L'entité banque

L'entité banque est une entité indépendante, mais relativement semblable à l'entité client. Deux centres de traitement, notamment «Gérer les adhésions» (Fig. 4.7) et «Vérifier les billets» (Fig. 4.8) sont uniques à cette entité. Par contre, les centres de traitement des transactions et des communications sont, à quelque sous-modules près, identiques à ceux du client. C'est pour cette raison que plusieurs modules et sous-modules se trouvant dans le DFD de l'entité client se retrouvent aussi – avec la même numérotation, pour indiquer qu'il s'agit bien du même module ou sous-module, respectivement – dans le DFD de l'entité banque.

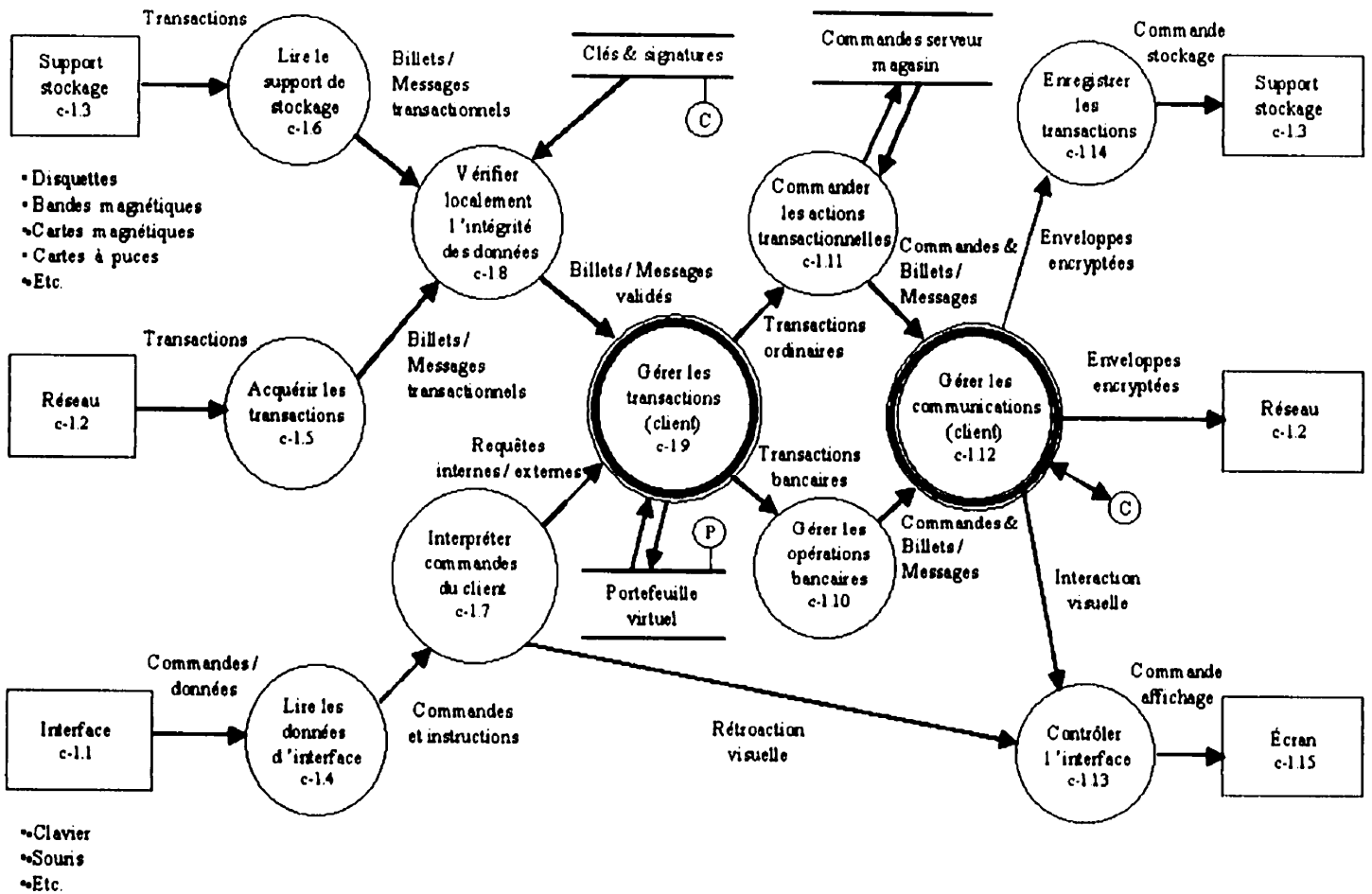

Figure 4.3 – *Le DFD de l'entité client – premier niveau de raffinement*

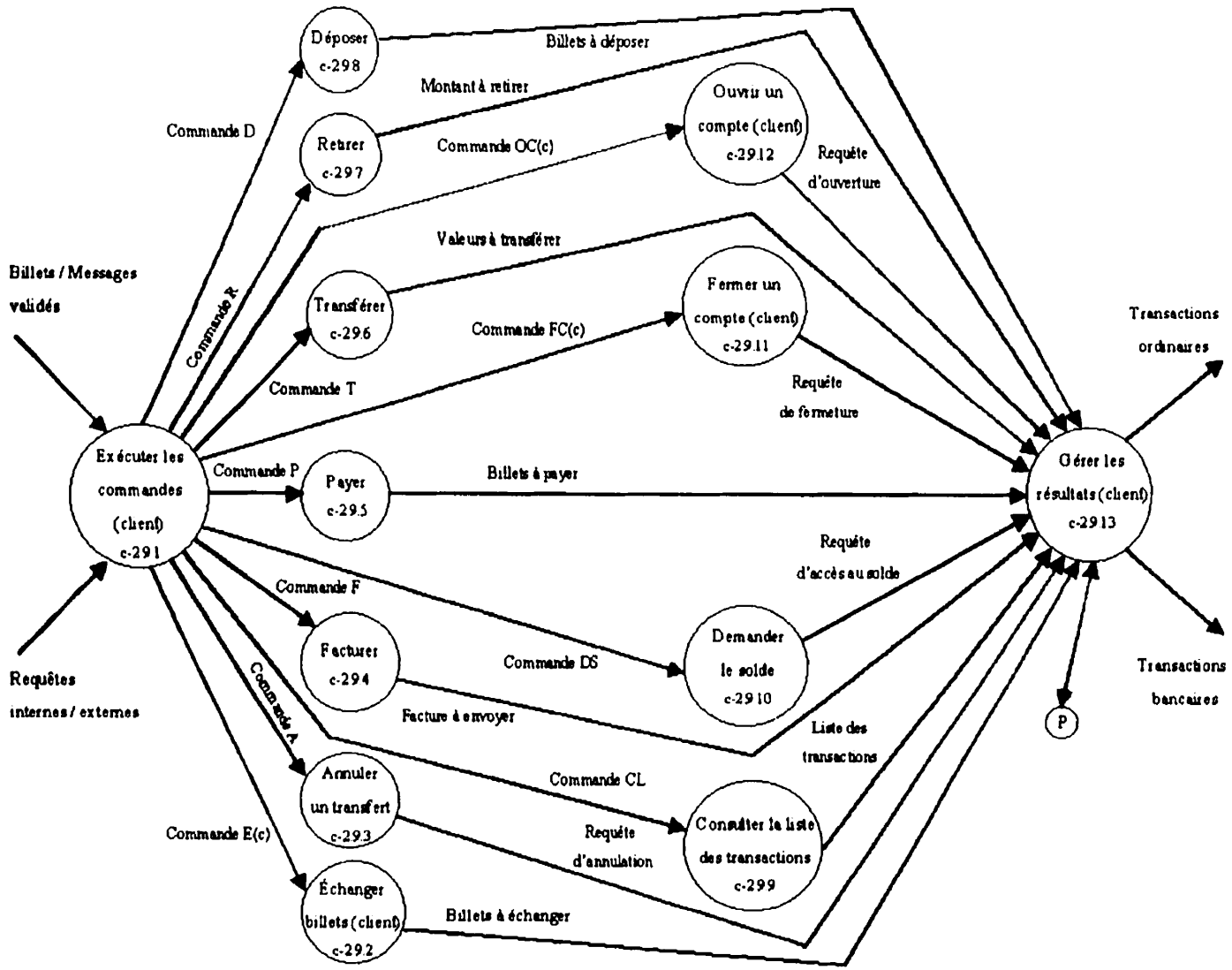

Figure 4.4 – *Le DFD de l'entité client – deuxième niveau de raffinement: le centre de traitement «Gérer les transactions (client)»*

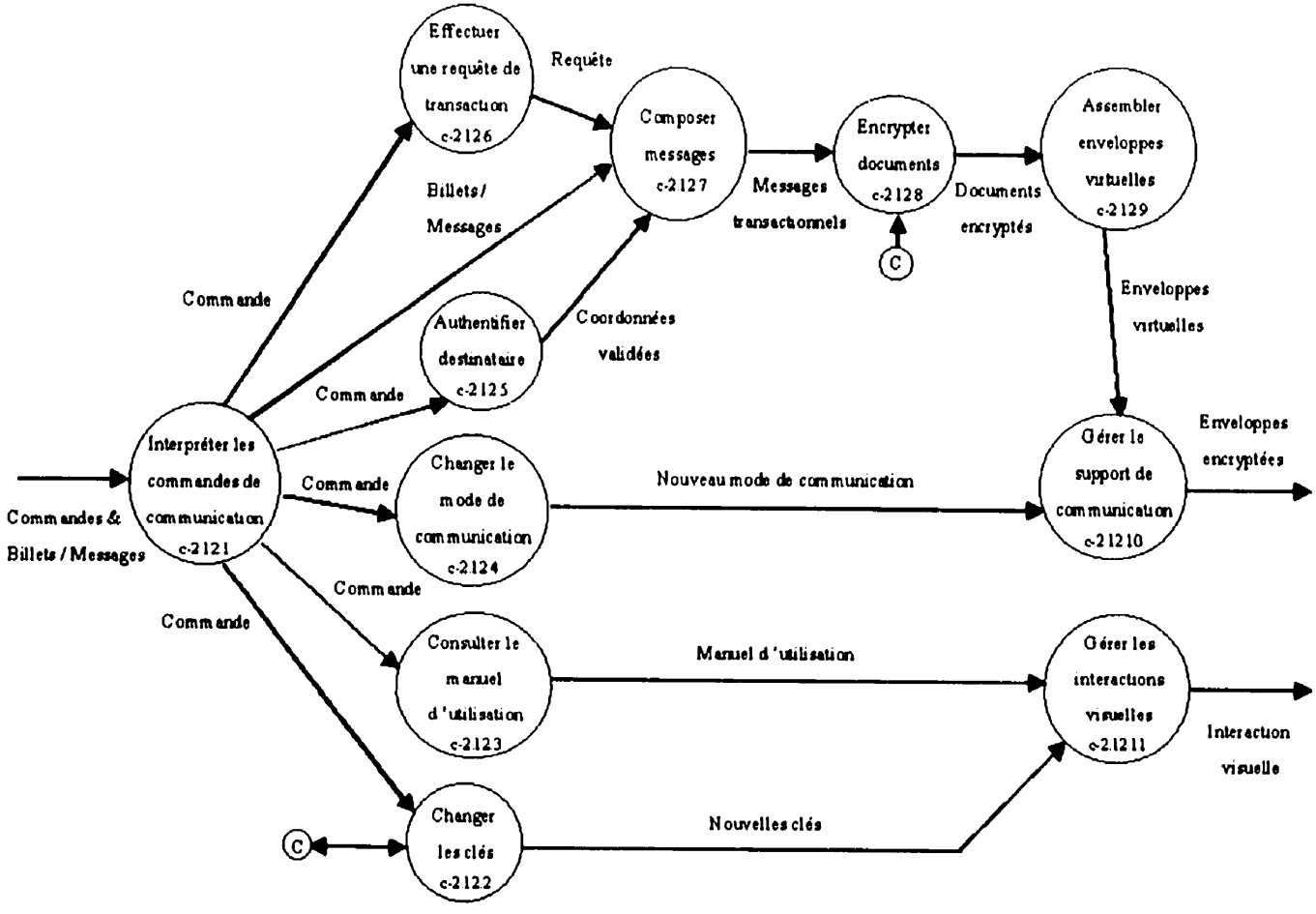

Figure 4.5 – *Le DFD de l'entité client – deuxième niveau de raffinement: le centre de traitement «Gérer les communications (client)»*

Les entrées des données transactionnelles et des données d'interface, ainsi que les modules permettant leur lecture, sont identiques à ceux de l'entité client. Deux entrées additionnelles sont présentes ici toutefois, soit un numériseur et un générateur de nombres aléatoires[2]. Les sorties de l'entité banque sont identiques à celles de l'entité client.

À part la gestion des clés biométriques (à l'aide du module b-1.7), quatre autres fonctions vitales sont propres à l'entité banque, notamment les modules b-1.8 «Gérer les comptes» et b-1.11 «Émettre des billets», ainsi que les centres de traitement b-1.5 «Gérer les adhésions» et b-1.6 «Vérifier les billets». En fonction de l'application concrète pour laquelle le système sera utilisé, ces fonctions pourront être employées pour effectuer des opérations légèrement différentes – par exemple, l'émission des billets pouvant être remplacée par la certification des documents.

Quatre centres de traitement sont détaillés dans le DFD de l'entité banque. Tout d'abord le centre «Gérer les adhésions» est développé à la Figure 4.7. C'est à l'aide de ces sous-modules que les images des signatures manuscrites sont traitées, les ID-biométriques sont formés et les nouveaux comptes sont générés. Nous y reviendrons à la section 4.4.

La Figure 4.8 montre les détails du centre de traitement «Vérifier les billets», centre qui permet de contrôler non seulement l'intégrité des documents numériques, messages transactionnels ou billets virtuels transigés, mais aussi d'assurer la protection contre d'autres types de fraude, notamment celle par copiage. Ainsi, une fois les enveloppes virtuelles désassemblées (dans le module b-2.6.1), les messages transactionnels sont décryptés et décomposés (dans les modules b-2.6.2 et b-2.6.3, respectivement). Ces opérations permettent par elles-mêmes de vérifier l'intégrité des

[2] La description complète des E/S sera présentée dans la section suivante portant sur le design préliminaire.

enveloppes, des messages et des champs constituants, opérations nécessaires non seulement pour les paiements électroniques mais aussi pour les autres types de transfert et d'échange de valeurs.

Notons que le sous-module b-2.6.8 «Retrouver faussaire» est un «pseudo-sous-module», dans le sens qu'il n'appartient pas en tant que module logiciel à l'entité banque. Il s'agit plutôt d'un ensemble d'actions qui doivent être prises par la banque, en coopération avec d'autres organismes et institutions, afin d'assurer un niveau de dissuasion suffisant pour décourager les fraudes et protéger ainsi la qualité de la RM et des valeurs véhiculées par le système. C'est pour cette raison qu'il n'y a pas de sortie d'interface marquée sur le DFD, car l'ensemble des actions à prendre dépend totalement des politiques internes de l'émetteur.

En ce qui concerne les paiements, le cœur du centre de vérification «Vérifier les billets» est constitué par le sous-module b-2.6.4 «Comparer numéro de série», qui permet la protection tant pour les transactions en-ligne que pour celles hors-ligne. Suivant le résultat généré par ce sous-module, des actions différentes seront entreprises par l'entité banque, qui assure ainsi la protection et la qualité de sa RM.

Regardons enfin les deux autres centres de traitement. Il est relativement facile de remarquer que les centres de l'entité banque qui s'occupent du traitement des transactions «Gérer les transactions» (b-1.9 dans Fig. 4.6, explosé dans Fig. 4.9) et de la gestion des communications «Gérer les communications» (b-1.12 dans Fig. 4.6, explosé dans Fig. 4.10) ressemblent fortement aux centres ayant les mêmes fonctions de l'entité client.

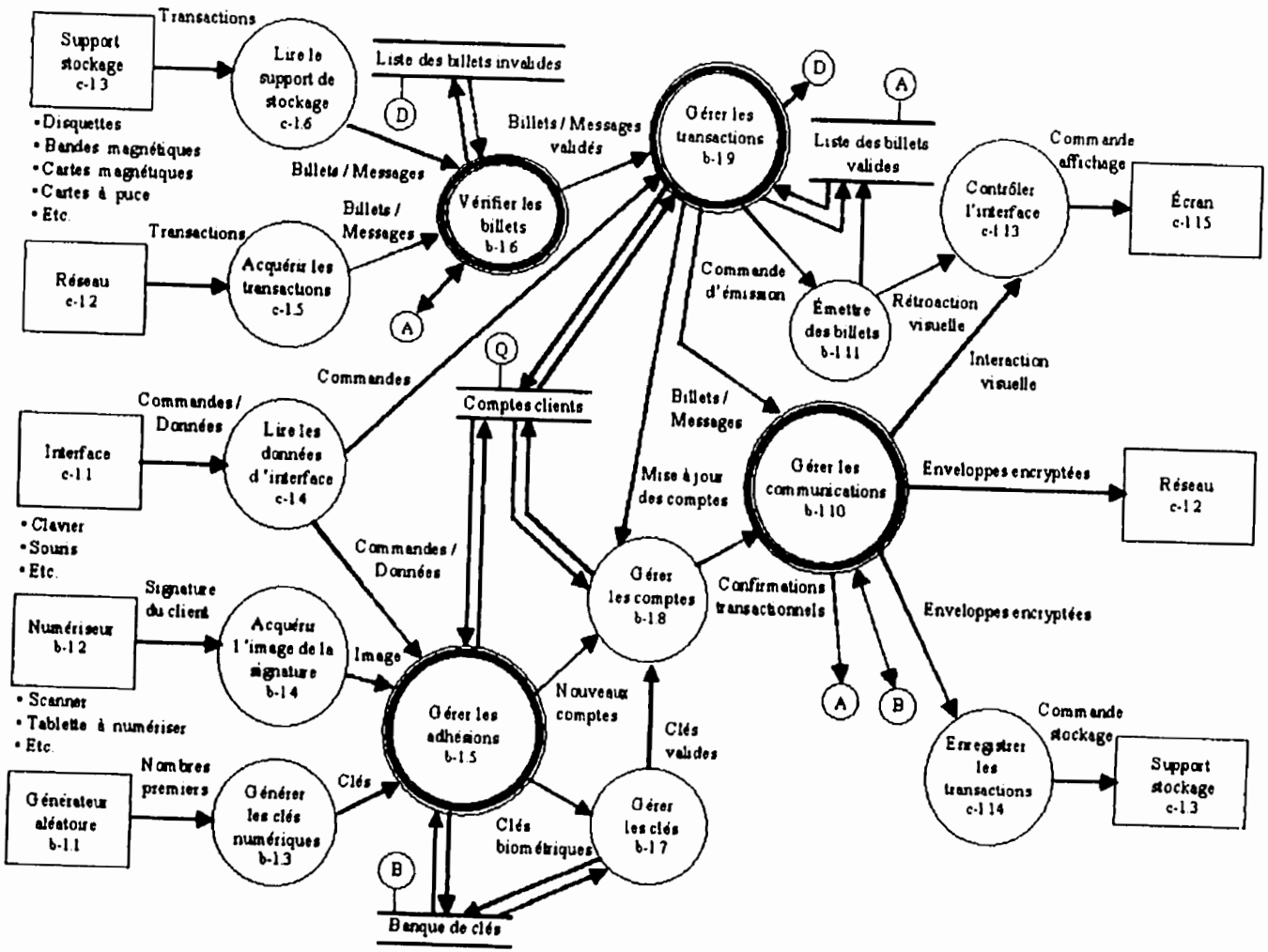

Figure 4.6 – *Le DFD de l'entité banque – premier niveau de raffinement*

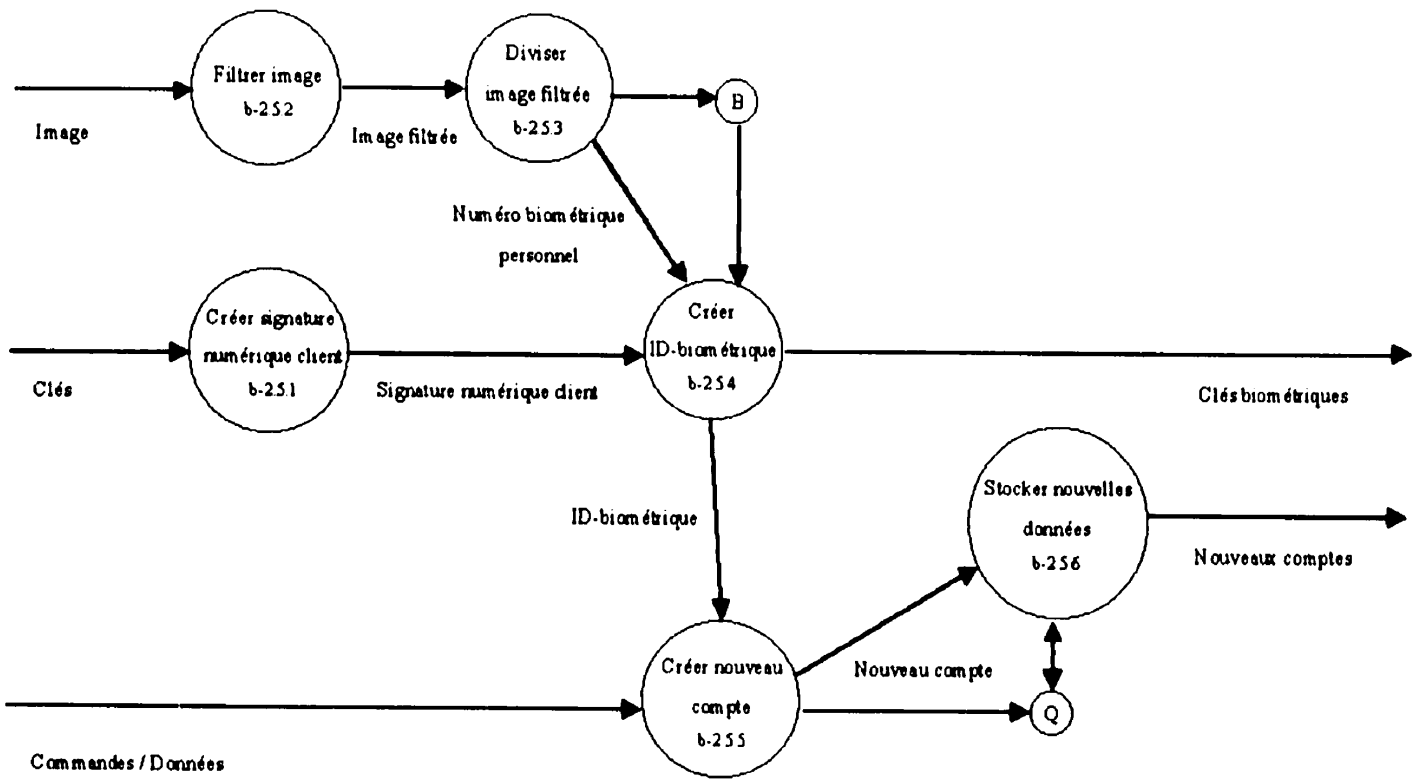

Figure 4.7 – *Le DFD de l'entité banque – deuxième niveau de raffinement: le centre de traitement «Gérer les adhésions»*

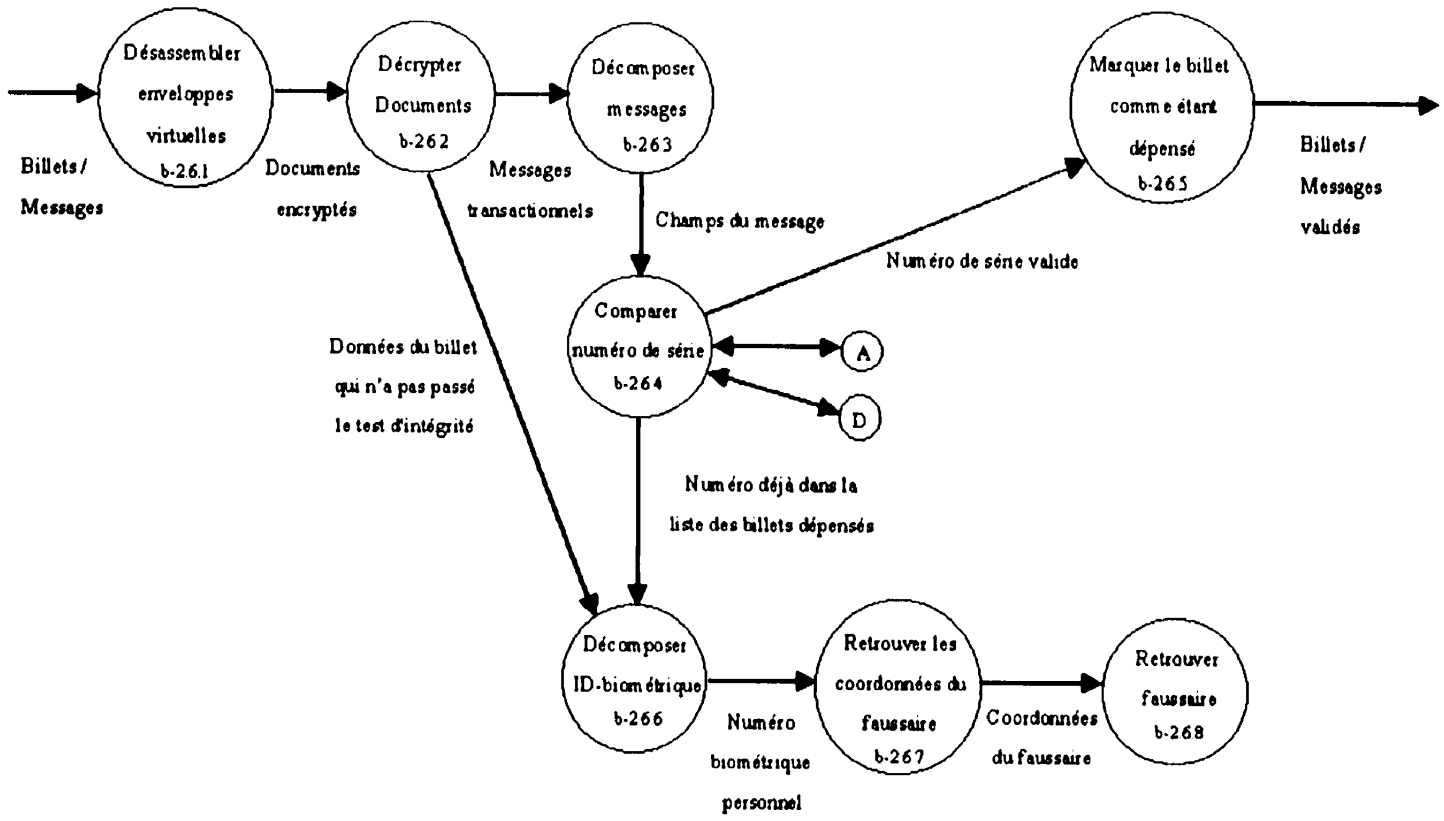

Figure 4.8 – *Le DFD de l'entité banque – deuxième niveau de raffinement: le centre de traitement «Vérifier les billets»*

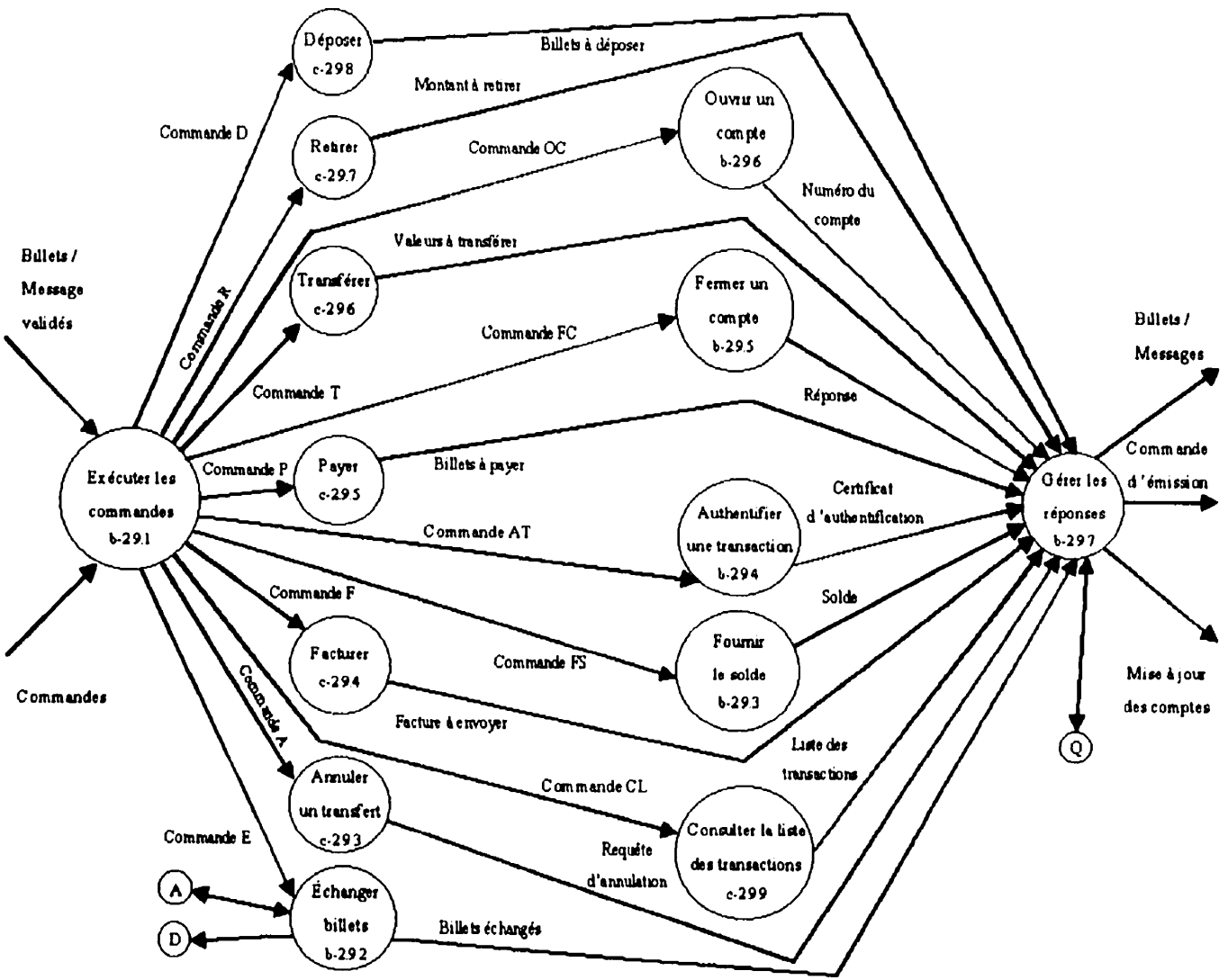

Figure 4.9 – *Le DFD de l'entité banque – deuxième niveau de raffinement: le centre de traitement «Gérer les transactions»*

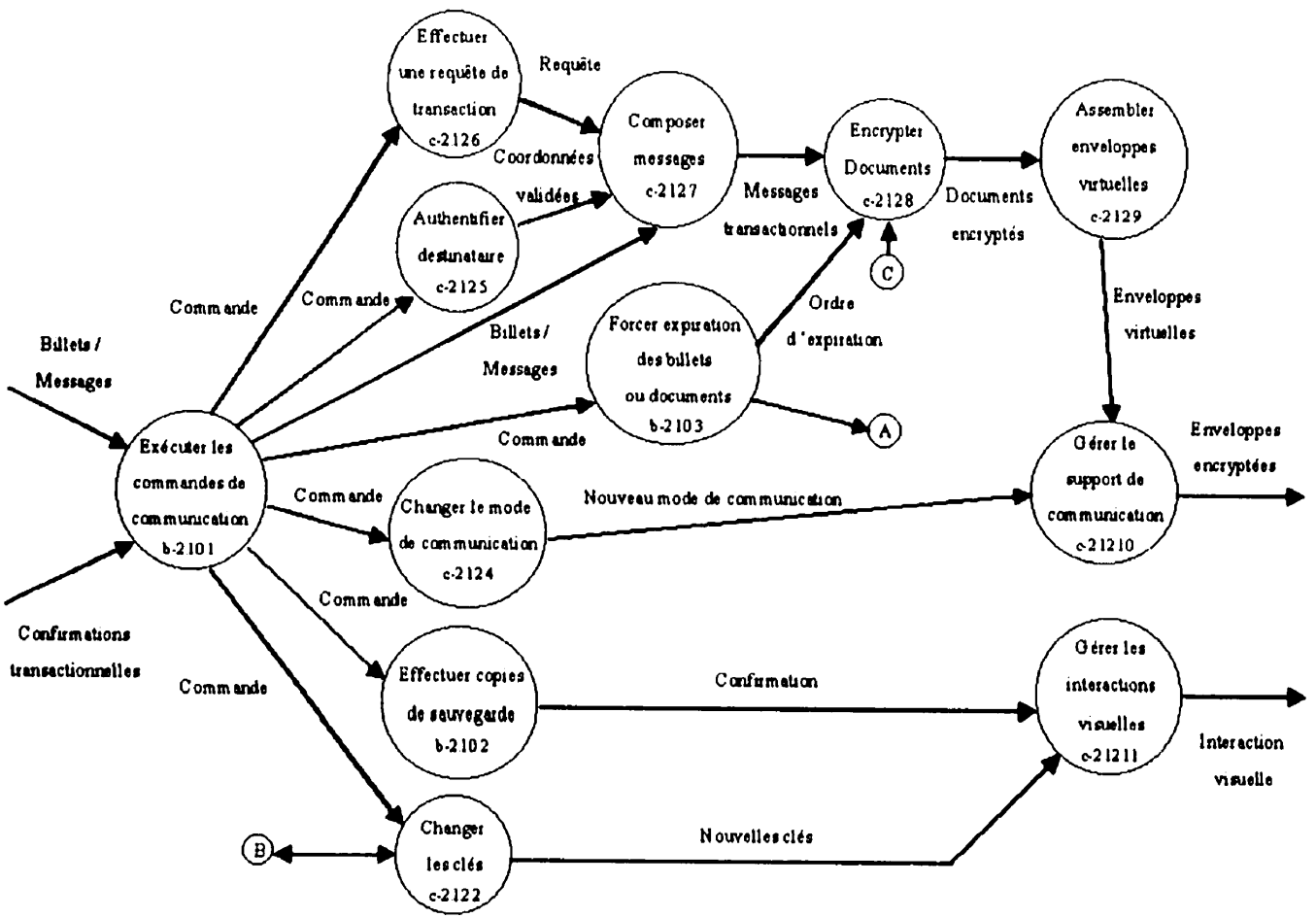

Figure 4.10 – *Le DFD de l'entité banque – deuxième niveau de raffinement: le centre de traitement «Gérer les communications»*

C'est une des raisons pour lesquelles l'entité client permet d'effectuer la certification de documents électroniques et d'autres valeurs numériques. Dans ces deux centres de traitement, des sous-modules spécialisés permettent d'effectuer des opérations reliées aux fonctions propres aux émetteurs, telles que l'authentification des transactions (billets, documents, etc., par l'intermédiaire du module b-2.9.4) ou l'expiration forcée des billets ou des certificats qui accompagnent les objets virtuels émis (à l'aide du module b-2.10.3).

Voilà donc les détails fonctionnels, à deux niveaux de raffinement, de chacune des deux parties constituantes de TRANZIX. À partir du DFD que nous venons de présenter, nous allons construire la hiérarchisation des modules, dans la section suivante.

4.3 Design préliminaire

Nous allons présenter dans cette section le design préliminaire du système électronique de transfert numérique de valeurs, tant pour l'entité client que pour la l'entité banque, telles qu'elles ont été définies dans les spécifications fonctionnelles. Le but du design préliminaire est définir une méthode permettant une approche systématique pour le développement et la documentation de la structure d'un système, à partir du diagramme de flux de données défini lors de l'étape de conception des spécifications fonctionnelles. Nous allons donc déterminer la structure et l'architecture d'un nouveau système de transfert de valeurs en définissant la hiérarchie des modules, les moyens de communication du système avec son environnement, ainsi que les données véhiculées par TRANZIX.

Concrètement, dans un premier temps, nous allons introduire, à partir du DFD présenté dans la section précédente, le diagramme hiérarchique général de chaque entité. Par la suite, nous allons énumérer les interfaces d'E/S du système et en regardant brièvement leurs rôles. Enfin, nous allons déterminer la structure des données qui circulent dans le système et spécifier les composantes de chaque type de donnée présent.

4.3.1 Le diagramme hiérarchique

Nous présentons dans les pages qui suivent le diagramme hiérarchique du système TRANZIX, diagramme qui décrit séparément – lui aussi – la partie client de la partie banque. Le DH décrit les grandes lignes de chaque entité en montrant la hiérarchie des modules composants. Ainsi, la Figure 4.11 présente la hiérarchisation des modules de la partie client; les modules correspondent au DFD général de cette entité et possèdent donc la même numérotation. Au plus bas niveau de cette hiérarchie, nous avons placé les modules matériels, représentant les interfaces d'E/S.

Notons au niveau supérieur de cette structure l'ajout de trois «pseudo-modules», sans numérotation propre, qui servent à départager les modules traitant les différents types de flux de données. De cette manière, le pseudo-module «Acquérir les entrées» permet de traiter le flux afférent des données, tandis que le traitement du flux efférent est effectué par le pseudo-module «Contrôler les sorties (client)».

En ce qui concerne la partie banque, la Figure 4.12 démontre clairement les différences entre les deux entités au niveau du traitement des données, mais aussi les ressemblances au niveau de l'acquisition des entrées et du contrôle des sorties. Plus précisément, notons que le traitement du flux afférent est identique dans les deux entités et que le traitement du flux efférent est relativement semblable dans les deux cas.

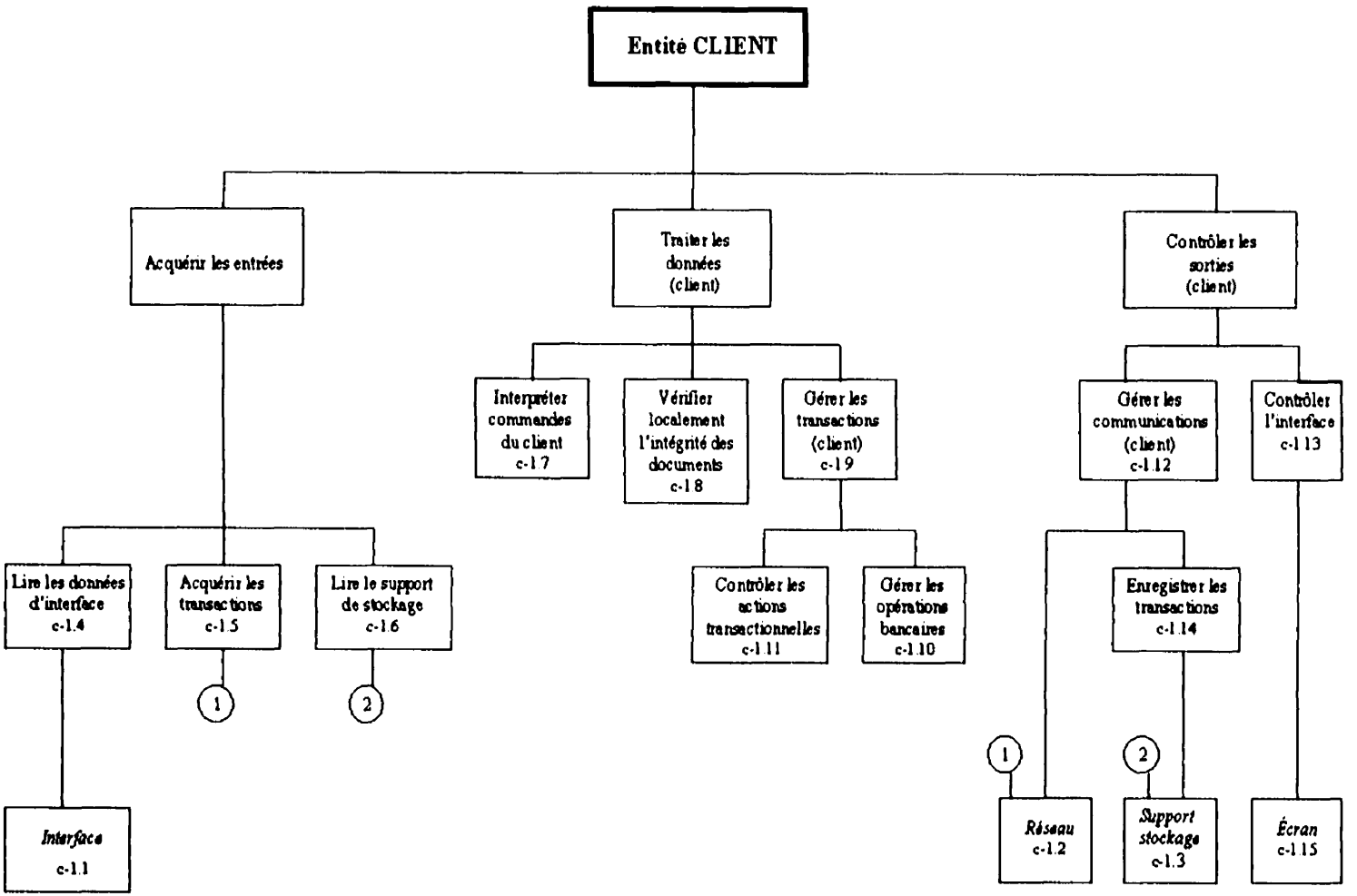

Figure 4.11 – *Le DH de l'entité client*

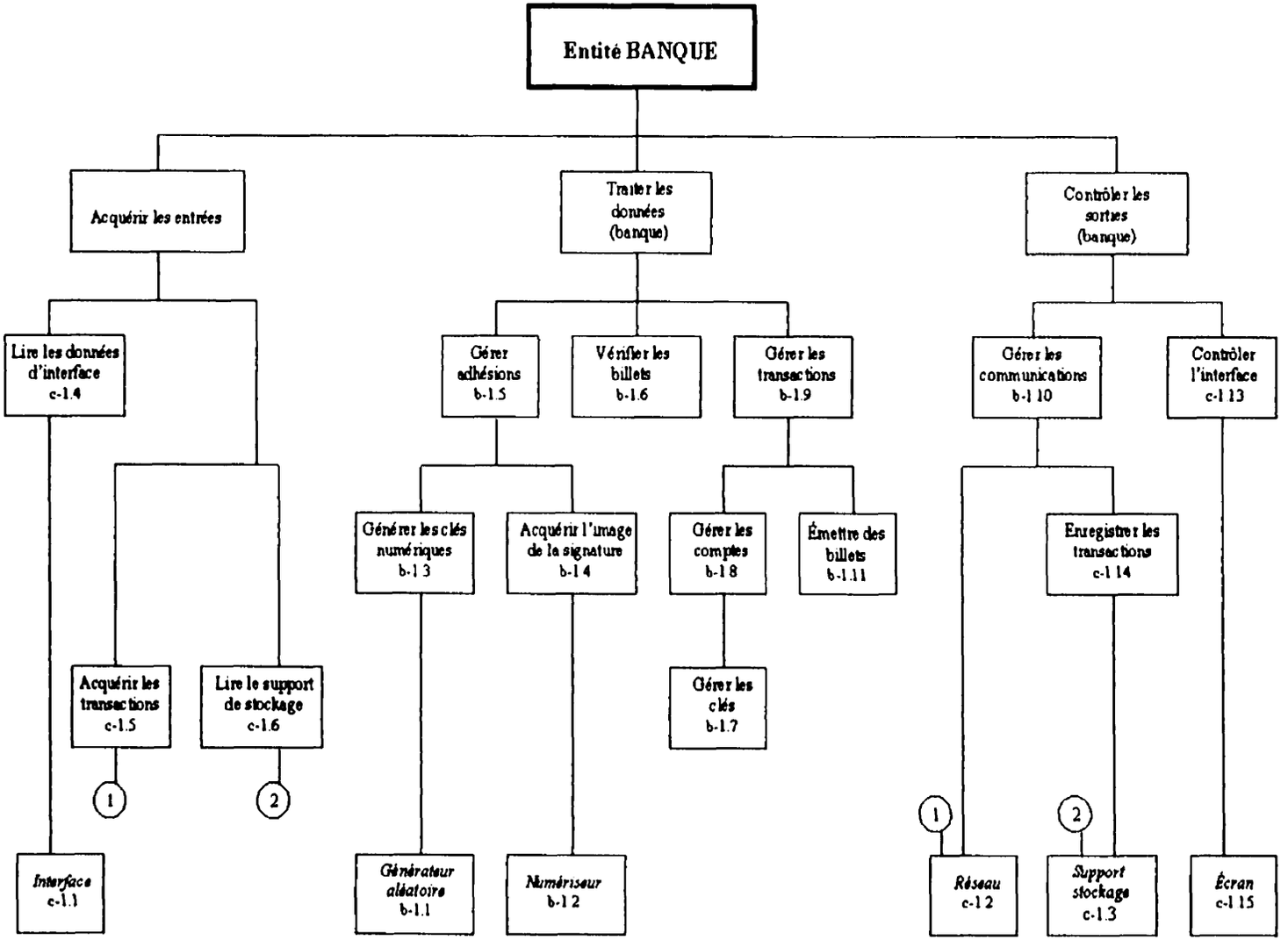

Figure 4.12 – *Le DH de l'entité banque*

4.3.2 Description des interfaces

Le système électronique de transfert numérique généralisé de valeurs peut être vu globalement comme un système quasi fermé, avec un nombre relativement réduit d'E/S. Tel qu'indiqué dans le DFD, les entrées et les sorties du système sont les suivantes:

- ***l'interface***: il s'agit de l'interface du logiciel du client et de celui de la banque avec l'environnement extérieur. Elle permet aux utilisateurs de chaque entité d'entrer des données – qu'elles soient des instructions, de commandes ou autres. L'interface comprend un clavier ordinaire qui accompagne tout ordinateur personnel et une souris, autre unité matérielle bien connue, servant à entrer des commandes et requêtes en mode graphique;

- ***l'écran***: unité standard, qui accompagne habituellement un ordinateur personnel, servant à l'affichage des rétroactions visuelles; les utilisateurs peuvent ainsi visualiser de façon interactive toute requête, réponse ou travail en cours;

- ***le réseau*** de communication: sert de support physique de communication entre les différentes entités du système; le réseau doit utiliser un protocole de communication compatible avec le protocole TCP/IP, en l'occurrence, tout sous-réseau d'Internet. De façon pratique, la connexion entre un ordinateur et le réseau de communication est réalisée par l'intermédiaire de tout équipement de branchement, tel qu'un modem compatible avec les normes V32, V32bis, V34, etc.;

- ***le support de stockage***: permet d'emmagasiner des documents électroniques ou des billets numériques ainsi que d'autres messages transactionnels ayant la forme de fichiers binaires encryptés. Il peut être constitué par tout support physique capable de stocker ou de transporter des données numériques – disquette, disque rigide, bande magnétique, carte magnétique, carte à puce, etc. Le support matériel doit être muni d'un pilote (*driver*) approprié ainsi que du logiciel de gestion nécessaire à son bon fonctionnement et à son interface avec l'ordinateur;

- ***le numériseur***: un module matériel indépendant ou intégré dans une autre application matérielle, telle qu'une tablette à numériser, servant à numériser un document sur papier – notamment les demandes d'adhésion et ouverture de compte, contenant les signatures manuscrites des clients – afin de les transformer en format binaire. De préférence, cet appareil sera un numériseur, de moyenne ou haute résolution – préférablement au moins 150 dpi (points par pouce);

- ***le générateur aléatoire***: permet la génération de nombres aléatoires qui seront utilisés pour construire des clés numériques à l'aide d'un protocole de génération de clés d'un algorithme cryptographique d'encryptage asymétrique. Cet algorithme permettra aussi l'utilisation de clés privées pour générer des signatures numériques. Physiquement, le générateur pourra créer des nombres pseudo-aléatoires à l'aide d'un module matériel ou d'un mécanisme logiciel ou mixte, tel que `/dev/random` sur certaines systèmes d'opération UNIX.

Remarquons que ni le client ni le vendeur n'a besoin d'équipements matériels additionnels. Seule l'entité banque utilisera des équipements matériels spécifiques, soit un numériseur (scanner, tablette à numériser, etc.) capable de numériser les images des documents sur papier contenant des signatures manuscrites.

4.3.3 La structure des données

Nous allons définir dans cette sous-section, de façon précise, la structure des données qui circulent dans le système, en spécifiant leur composition et leurs particularités. Il est important de remarquer dès le début qu'il existe une redondance contrôlée de la plupart des données véhiculées, aussi bien dans la base de données de la banque que dans les portefeuilles virtuels des clients, afin d'augmenter le niveau de sécurité et de confiance dans le système. Ainsi, des copies des transactions sont gardées par toutes les entités concernées et une copie de sauvegarde de tout message transactionnel de haut niveau, qu'il soit un document électronique ou un billet numérique, est gardée de façon transparente dans le portefeuille virtuel de l'usager jusqu'à la conclusion finale de la transaction.

Nous avons classifié les données circulant dans le système en quatre types différents que nous allons énumérer et décrire en détail dans les pages qui suivent:

1. Les messages informatifs;
2. Les enveloppes virtuelles;
3. Les coordonnées d'identification des clients;
4. Les comptes bancaires.

4.3.3.1 Les messages informatifs

Les messages informatifs sont constitués par les échanges de requêtes, commandes ou données entre le client et le serveur de communication, dans les deux entités transactionnelles, pour établir, garder ou interrompre une communication, ainsi que pour demander ou fournir des informations de haut ou bas niveau. Ainsi, les ***informations de bas niveau*** (ou ***messages de contrôle***) sont les informations qui servent à mettre en place le protocole transactionnel TRANZIX – par exemple, les prises de contact (*handshakes*) pour établir une connexion. Il faut mentionner qu'il ne s'agit pas ici de simples échanges d'information utilisés par le protocole de communication TCP/IP, mais plutôt de messages du protocole d'échange numérique de valeurs.

Les ***informations de haut niveau*** sont les informations «utiles» – demandes ou réponses – regardant, par exemple, l'état de la connexion, de statut d'une transaction, etc. De façon générale, chaque message contient les champs suivants, tel que présenté à la Figure 4.13:

- champs de contrôle;
- type de message;
- destinataire;
- expéditeur;
- charge utile.

Les mnémoniques utilisées dans la Figure 4.13 sont les suivantes:

- CTRL-DEBF = Contrôle du message – Début du fichier;
- CTRL-FINF = Contrôle du message – Fin du fichier (contient aussi une somme de vérification du fichier);

- TYPE = Type du fichier / message; Valeurs possibles:
  - MB = Message émis par l'entité banque;
  - MC = Message émis par l'entité client;
  - DB = Document électronique émis par l'entité banque;
  - DC = Document électronique émis par l'entité client;
  - BV = Billet virtuel, au porteur;
  - MP = Mandat pour paiement unique;
  - RR = Billet récupéré après une défaillance;
- DEST = Destinataire du message;
- EXPD = Expéditeur du message;
- UTIL = Charge utile.

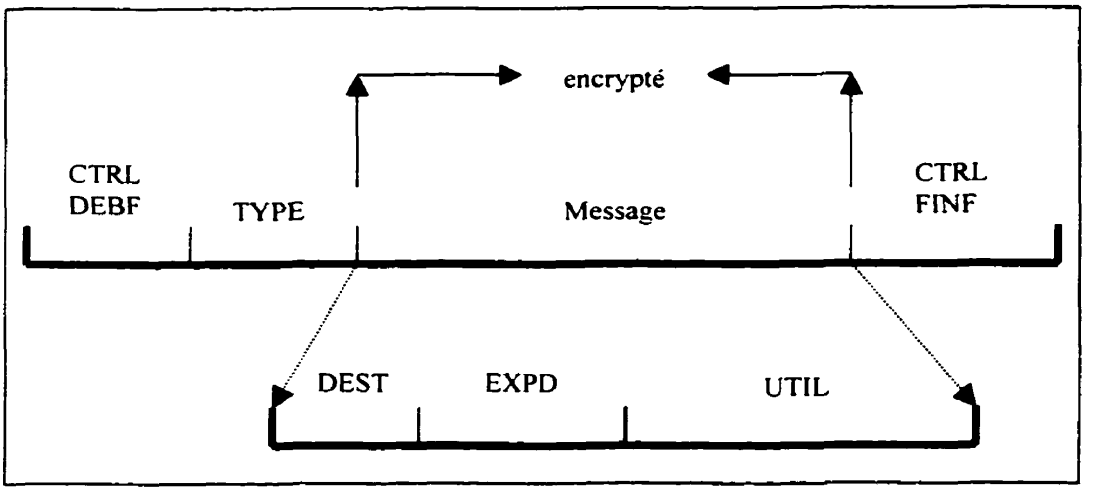

Figure 4.13 – *La structure des champs d'un message informatif*

4.3.3.2 Les enveloppes virtuelles

Nous allons nous attarder un peu plus sur ce type de données, puisqu'elle constitue un aspect primordial du système TRANZIX. Trois sous-types d'information

peuvent être contenus dans chaque enveloppe virtuelle, soit l'information utile, l'information de contrôle et le champ de remplissage.

L'***information utile*** est constituée par les données qui permettent de façon intrinsèque de transporter la valeur, d'un point à un autre, numériquement. Ces données sont importantes: elles ont une valeur économique et sont confidentielles; elles doivent donc être protégées, tant contre les erreurs de transmission, les erreurs de fonctionnement, que contre les fraudes éventuelles. La charge utile peut être constituée, comme nous l'avons vu dans le Chapitre 3, par n'importe quel objet virtuel ayant une valeur non-intrinsèque quelconque: de l'argent, des certificats, des documents – tels qu'un permis de conduire, une carte d'assurance santé, un diplôme d'études –, etc.

Pour contrôler l'intégrité de l'information utile, nous allons utiliser une certaine quantité d'***information de contrôle***, redondante ou non. Ces informations sont distribuées dans plusieurs champs du fichier binaire représentant l'enveloppe, notamment pour marquer le début et la fin du fichier, ainsi que la vérification de somme (*checksum*) du fichier.

Toutefois, ce type de contrôle n'est pas toujours suffisant pour assurer la confidentialité des informations utiles, surtout contre les méthodes de décryptage utilisant l'analyse du trafic. Nous introduisons alors un champ supplémentaire, de longueur variable, qui contient des bits de ***remplissage***, sans valeur informative. Ce champ permettra de dissimuler l'endroit où l'information utile se trouve, ou, de façon optionnelle, de changer même la longueur du fichier représentant l'enveloppe, pour chaque enveloppe virtuelle, séparément.

La structure des enveloppes est identique à celle des messages informatifs, présentés dans la Figure 4.13. Le champ UTIL, contenant l'information utile, devient l'endroit où le contenu de l'enveloppe est placé. Un marqueur contenant l'emplacement

du début ainsi que la longueur du champ de remplissage est une information de contrôle placée au début de la charge utile. Ces informations n'affaiblissent pas la sécurité du système, car elles sont encryptées tout comme le reste de la charge utile.

4.3.3.3 Les coordonnées d'identification des clients

Comme dans beaucoup d'autres applications, surtout financières, des coordonnées détaillées d'identification des clients sont nécessaires pour enregistrer chaque usager du système et ainsi les protéger. À l'aide de ces informations, les clients peuvent être protégés contre toute erreur de fonctionnement ou de communication et contre toute fraude par copiage, contrefaçon ou double-dépense – soit par prévention, soit par vérification immédiate ou différée, ainsi que par dissuasion, en poursuivant en justice la personne qui a été détectée comme fraudeur.

Toutes les autres informations demandées aux clients, qui se trouveront éventuellement dans la base de données de l'émetteur sont protégées par encryptage. De plus, ces informations sont protégées conformément aux lois en vigueur concernant les renseignements personnels, comme dans tout autre établissement financier, et pourront inclure pour chaque client – en fonction de la politique de chaque émetteur:

- le nom et prénom;
- la date de naissance;
- le numéro d'assurance sociale ou d'autres pièces d'identité;
- la clé publique;
- l'ID-biométrique;
- le revenu et les références financières;
- l'adresse et numéro de téléphone;
- l'adresse de courrier électronique;
- etc.

Lors de l'adhésion, les clients reçoivent un numéro de compte, qui servira aussi comme numéro d'identification, accompagné de la signature biométrique. Pour ce faire, lors de la génération des clés cryptographiques, le client gardera sa clé privée dans son portefeuille virtuel et donnera à la banque une copie de sa clé publique afin qu'elle puisse lui envoyer des messages transactionnels encryptés.

Toutes ces informations seront mises dans des tableaux ayant des cases de longueur fixe pour chaque champ, afin de simplifier et alléger au maximum les structures internes de données. Tous les tableaux seront encryptés à l'aide d'un chiffre symétrique, tel que IDEA, et peuvent être accédés en mode sécuritaire à l'aide d'une procédure de décryptage temporaire. Notons, cependant, que ces éléments de l'entité banque ne sont pas inclus dans notre design mais pourraient être ajoutés lors d'une phase de développement plus avancée.

4.3.3.4 Les comptes bancaires

Les comptes bancaires des clients constituent un type distinct de données, ayant la particularité de ne «circuler» que dans la partie banque – pour protéger les informations confidentielles des usagers et pour minimiser les risques de fraude. Ces données incluent:

- les comptes des usagers (numéros, contenu et soldes);
- une base de données «analogiques» contenant les formulaires sur papier de demande d'ouverture de compte avec les signatures des clients;
- une base de données «numériques» contenant les coordonnées de chaque détenteur de compte, incluant sa clé électronique publique et – de façon partielle, comme nous allons voir dans la sous-section 4.4.4 – l'image numérisée de sa signature manuscrite;

- la liste des numéros de série des billets déjà déposés ou invalides; elle inclut une sous-liste des paiements contenant des billets potentiellement faux (à vérifier plus en détail par les employés de la banque). La liste des billets invalides sert aussi comme «babillard électronique» pouvant être, de façon optionnelle, téléchargé périodiquement et consulté par les clients, afin de renforcer leur capacité de vérification locale;
- la liste des numéros de série des billets en circulation ou valides; cette liste inclut séparément une trésorerie virtuelle contenant des billets neufs, à mettre en circulation, ainsi qu'une trésorerie virtuelle contenant des billets appartenant à d'autres émetteurs, en attente du processus d'acquittement et de clearing interbancaire.

Tout comme les autres données d'identification, ces structures seront construites et utilisées de façon à alléger et à simplifier au maximum le fonctionnement du système. Ainsi, ces structures pourront utiliser des tableaux de pointeurs, ayant des cases de longueur fixe, donc les données seront placées à des espaces égaux dans la mémoire volatile ou sur le support de stockage.

4.4 La protection du système

Cette avant-dernière section du Chapitre 4 est consacrée aux différents aspects concernant la protection du système TRANZIX. Nous allons présenter les moyens qui permettent de traiter les différents types d'exceptions ainsi que de sécuriser les communications et de protéger les émetteurs et les usagers. Nous allons décrire comment les moyens cryptographiques permettent d'assurer au système un très haut

niveau de confidentialité et d'intégrité et comment renforcer l'authenticité et la non-répudiation des transactions en personnalisant les billets et les autres valeurs transigibles à l'aide de moyens biométriques.

4.4.1 Le traitement des exceptions

Afin de parer à toutes éventualités et préparer ainsi une meilleure prévention contre les éventuelles erreurs, nous allons anticiper dans cette sous-section les cas d'exception au fonctionnement normal, qu'il s'agisse d'une irrégularité due au système ou causée par les entités transactionnelles. Concrètement, il y a d'une part les cas de fonctionnement défectueux ou de panne et, d'une autre part, il y a les cas de fraude de différents types. Le traitement des exceptions est effectué de manière distribuée, chaque entité ayant ses capacités de vérification implantées dans son logiciel et ses responsabilités de sauvegarde et recouvrement – responsabilités fortement recommandées.

4.4.1.1 Les erreurs de fonctionnement

En regardant les spécifications fonctionnelles, deux types d'erreurs pourraient apparaître: les erreurs de transmission et celles de fonctionnement. Dans le premier cas, les données transmises sur le réseau sont affectées par un problème potentiel de communication, tandis que, dans le deuxième, l'erreur pourrait être causée soit par un mauvais fonctionnement de l'équipement matériel des usagers (clients ou banques), soit par une défaillance du logiciel.

Les erreurs de transmission sont détectées en vérifiant tout d'abord la présence et l'ordre des messages de contrôle de bas niveau du protocole transactionnel, ainsi que des champs constituants des messages et des enveloppes virtuelles. Par la

suite, la vérification de l'intégrité des deux champs de contrôle, CTRL-DEBF et CTRL-FINF, est effectuée; ce dernier champ de contrôle contient un marqueur ainsi qu'une vérification de somme (*checksum*) qui peut être contrôlée en la recalculant après l'arrivée du fichier à sa destination. Ceci n'est d'ailleurs qu'une vérification additionnelle – servant à accroître le niveau de sécurité –, étant donné que la vérification de la rectitude de la transmission est effectuée déjà par le protocole de communication TCP, ainsi qu'à un plus bas niveau par le protocole IP.

Le cas d'une défaillance de fonctionnement – matériel ou logiciel – est traité de façon à protéger tout d'abord les clients. En ce qui concerne le matériel, une éventuelle erreur de fonctionnement ne relève pas de notre système. Pour ce qui est des modules logiciels, notons que le langage Java offre des structures d'instructions dédiées aux exceptions, permettant de détecter différents types d'erreurs ainsi que des «erreurs générales ou imprévues» qui sont engendrées par un défaut inopiné de fonctionnement ou d'utilisation et qui pourrait avoir une cause difficile à identifier.

Des copies temporaires des informations vitales, ainsi que des objets virtuels transigés – particulièrement des billets – sont effectuées de manière transparente par le système et sont gardées jusqu'à la finalisation complète de toute transaction. Des copies additionnelles de sauvegarde, utilisant des supports différents et indépendants, peuvent être suggérées aux usagers. Ces copies représentent la manière la plus sûre et la plus efficace pour se prémunir contre tout imprévu. De cette façon, les usagers pourront recouvrir leurs données dans le cas d'une défaillance logicielle mais aussi dans le cas de défaillance matérielle majeure.

4.4.1.2 Les pannes

Les pannes, ces arrêts de fonctionnement accidentels et momentanés, sont des exceptions relativement proches des erreurs de fonctionnement. Regardons quelques

pannes qui pourraient éventuellement se produire dans le fonctionnement du système avec une probabilité suffisante pour les considérer ici. Une possibilité de panne existe toujours pour tout serveur de transactions. La meilleure solution dans le cas d'une panne de l'entité banque est la prévention. Si l'apparition d'une panne – ainsi que ses causes – est imprévisible, la perte totale et coûteuse d'informations peut toutefois être évitée en utilisant un serveur miroir, de remplacement, situé sur un autre ordinateur et préférablement dans un emplacement physiquement différent du serveur principal.

Dans le cas d'une interruption accidentelle ou intentionnée de la communication au milieu d'une transaction, celle-ci doit être reprise une fois la connexion rétablie. Le message transactionnel qui n'a pas été complètement reçu est ignoré et la transaction ne peut pas être conclue, sa retransmission immédiate ou ultérieure étant indispensable pour l'achèvement correct de l'opération transactionnelle. La transaction devient alors automatiquement en-ligne, dans le sens qu'un contact avec l'émetteur est absolument nécessaire afin de décider du statut de la transaction. En effet, en fonction de l'étape [du protocole transactionnel] à laquelle la transaction interrompue s'est rendue, l'objet virtuel transféré peut appartenir encore à l'expéditeur ou peut être déjà passé dans la propriété du destinataire. En contactant l'émetteur, la transaction peut être reprise, en annulant la représentation numérique de l'objet virtuel en question et en créant une nouvelle.

Le cas d'une défaillance majeure, telle qu'un «écrasement» de disque dur (le disque dur d'un ordinateur est, par exemple, égratigné et devient physiquement illisible) est plus délicat. Normalement, la perte du disque dur ou d'une disquette contenant de l'argent électronique ou d'autres valeurs équivaut avec la perte d'un portefeuille réel et l'argent, ainsi que le reste de son contenu, est donc perdu.

Toutefois, dans certains cas, l'argent, (ou au moins une partie) peut être récupéré par le système TRANZIX. Ainsi, les billets perdus qui provenaient directement

de la banque, suite à un retrait ou à une transaction en-ligne, peuvent être récupérés. La banque annulera leurs numéros de série et libérera de nouveaux billets à la place, ayant les mêmes numéros mais avec la valeur RR (Billet récupéré) dans le champ TYPE; ces billets peuvent être utilisés immédiatement et sans restriction par le client. Par contre, si la banque n'a aucune trace directe des billets, ceux-ci ayant été reçus suite à une transaction hors-ligne, et si le client n'a aucune copie de sauvegarde, les billets seront perdus, et les coûts de la perte seront donc encourus par le client (comme dans la vraie vie lorsqu'on perd son portefeuille).

De façon générale, les pertes encourues par un éventuel fonctionnement défectueux ou par une panne du système du client seront encourues par le client, à moins qu'il soit protégé avec des copies de sauvegarde. De la même façon, les pertes encourues par un éventuel fonctionnement défaillant ou par une panne du système de la banque seront encourues par la banque, si elle ne possède ni des copies de sauvetage ni les moyens de retracer ses propres transactions.

4.4.1.3 Les fraudes

Deux sortes de fraudes sont possibles: les fraudes externes, effectuées par les clients, ou encore plus dangereuses, les fraudes internes, effectuées par un ou plusieurs membres du personnel de la banque. Une combinaison des deux cas peut se produire lorsqu'il y a collusion entre deux ou plusieurs entités transactionnelles. Bien que la protection contre les fraudes sera expliquée en détail dans la section suivante, nous allons regarder brièvement ici les principaux éléments de traitement de ce type d'exception.

4.4.1.3.1 Les fraudes externes

Ce type de fraude comprend les tentatives de falsification des documents électroniques et notamment des billets virtuels, par copiage, décryptage, interception ou piratage des communications. La banque a la responsabilité de détecter les faux documents et les faux billets et prendre des mesures en conséquence.

La fraude par copiage, ou la double-dépense, est la fraude la plus facile à effectuer, étant donné que dans le monde virtuel, une copie équivaut à une simple commande. La fraude par copiage est évitée en utilisant un numéro de série et des identificateurs biométriques. Ainsi, dans le cas des transactions financières en-ligne, la banque peut détecter immédiatement un faux billet en comparant sur-le-champ le numéro de série du billet avec la liste des billets déjà dépensés ou invalides.

Dans le cas où le billet serait invalide, en employant les identificateurs biométriques et les coordonnées d'identification des clients, la banque peut dépister et poursuivre le coupable, qui devra en supporter les coûts. Dans le pire des cas, la banque peut décider soit de supporter elle-même ces coûts soit de le porter au compte du payeur de la transaction contenant le faux billet, qui supportera le coût en perdant le montant du billet. Pour les transactions hors-ligne, le même protocole sera suivi, à l'exception du fait que, au pire des cas, la banque pourrait décider que le dernier propriétaire du faux billet, celui qui va le déposer à la banque, en supportera le coût.

En ce qui concerne le décryptage, l'interception ou le piratage de la communication, le traitement de ces exceptions est réalisé en assurant un haut niveau de protection du système par l'emploi de moyens cryptographiques forts, comme nous allons le voir en détail dans la sous-section 4.4.3. La protection contre ce type de fraude est fortifiée davantage en utilisant une longueur satisfaisante des clés cryptographiques, ainsi qu'un mécanisme de protection contre l'analyse du trafic.

4.4.1.3.2 Les fraudes internes

Les fraudes internes sont reliées à l'abus des privilèges dont jouissent les membres du personnel de la banque émettrice. Il s'agit tout d'abord soit de la manipulation illégale des soldes des comptes (fraude qui sera traitée de la même façon que celle des comptes dans les banques du «monde réel»), soit de la manipulation des signatures de la banque. En effet, en possédant la clé privée de la banque, quelqu'un peut signer, authentifier, certifier ou émettre tout message transactionnel, document électronique ou billet numérique. Une éventuelle fraude interne apparaît donc lorsqu'un malfaiteur (interne) subtilise ou rend publiques les clés secrètes de la banque, permettant ainsi à des utilisateurs non-autorisés de certifier ou d'authentifier des documents électroniques ou d'autres objets virtuels et même d'émettre des billets.

Des moyens stricts et systématiques de sécurité et de prévention de la perte[3] des clés secrètes de la banque devront être instituées, par des méthodes de sécurité physique qui sortent du cadre de notre ouvrage. Afin de limiter encore plus les éventuels dommages, nous avons introduit une date d'expiration pour chaque billet, leur donnant ainsi une ***durée de vie limitée***. Ceci force tous les usagers à échanger périodiquement leurs billets non-déposés pour des billets neufs.

Ainsi, dans le cas où la confidentialité des clés secrètes de la banque a été compromise, la banque se réserve le droit d'annuler tout billet signé avec des clés générées après la date de la perte. En ce qui concerne les autres documents électroniques signés ou certifiés numériquement, étant donné que les signatures et les certificats numériques contiennent la date d'émission, ils n'ont pas besoin d'être retournés ou certifiés de nouveau, puisque tout document émis, signé ou certifié avant la date de la perte sera considéré comme valide, tandis que tout document émis, signé ou certifié après la date de la perte sera considéré comme invalide.

---

[3] Dans le sens de perte et divulgation du secret.

4.4.1.3.3 Les fraudes par collusion

Une manière très subtile d'effectuer des fraudes financières est basée sur l'utilisation illicite des informations confidentielles ou d'initiés[4] ainsi que la collusion entre différentes entités. De telles tentatives de fraude sont très difficiles à prévenir ou à empêcher, surtout dans un environnement transactionnel virtuel. Regardons quelques possibilités plus évidentes de collusion et quelles pourraient être leurs conséquences.

Tout d'abord, s'il y a collusion entre le vendeur et la banque, l'anonymat de l'acheteur est compromis. En effet, le vendeur peut transmettre à la banque les coordonnées électroniques de l'acheteur, lui permettant ainsi de suivre les transactions des clients.

Si la collusion a lieu entre l'acheteur et la banque, le vendeur pourrait être fraudé. En effet, la banque pourrait informer l'acheteur sur les billets retirés directement par le vendeur, qui sont présentement dans sa possession – ou en possession d'un autre usager qui n'a pas encore effectué son dépôt à la banque. L'acheteur pourrait alors payer le vendeur avec de tels billets et c'est ce dernier qui serait détecté comme faussaire lorsqu'il utilisera ces billets. Toutefois, notons le fait qu'en regardant les signatures numériques et les dates qui les accompagnent, la banque pourrait trouver le vrai coupable.

Enfin, s'il y a collusion entre l'acheteur et le vendeur, aucune conséquence financière ne se produit, à part la perte de l'anonymat du possesseur antérieur du billet. Par contre, la double-dépense n'est pas possible; en copiant le billet avant de le transférer au vendeur et en essayant de le déposer en même temps que lui, l'acheteur ne pourra tirer profit de sa copie, puisque les transactions sont enregistrées de façon séquentielle. En effet, même si deux transactions sont effectuées en même temps auprès

[4] Dans le «monde réel» ceci peut inclure, par exemple, les délits d'initiés.

de deux serveurs différents de la banque (serveurs de transaction se trouvant dans des endroits différents), ces serveurs accèdent à la base centrale de données – contenant la liste des billets dépensés – de façon séquentielle et non pas de façon concurrente (en parallèle) – afin de maintenir l'intégrité des bases des données de la banque; il est évident donc qu'une seule entité transactionnelle, soit le vendeur, soit l'acheteur, pourrait profiter du billet en question. De plus, ultérieurement, la banque pourra retracer l'auteur du copiage et le poursuivre conformément à ses politiques.

Notons que le problème de collusion existe aujourd'hui dans tout système transactionnel, incluant les systèmes bancaires de chaque pays. TRANZIX hérite ainsi des problèmes semblables et présente les mêmes risques et solutions que les autres systèmes transactionnels du «monde réel». Ainsi, nous considérons que la dissuasion est la meilleure arme dans la lutte contre ce type de fraude. En assurant des politiques appropriées, permettant de responsabiliser les intervenants impliqués, ainsi que des mécanismes de supervision stricte et régulière, les émetteurs et les banques peuvent réduire fortement les risques et les préjudices apportées par les fraudes basées sur la collusion.

4.4.2 Sécurité et personnalisation

Nous avons montré qu'une caractéristique intrinsèque d'une très grande importance dans tout système transactionnel est la sécurité. Pour bien calibrer la protection assurée par TRANZIX, nous avons employé les cinq sous-critères de sécurité définis dans le Chapitre 2: la disponibilité – ou le contrôle d'accès –, l'intégrité des messages transactionnels, la confidentialité des communications, l'authenticité des entités transactionnelles et la non-répudiation des transactions.

TRANZIX permet de relier la sécurité physique, la sécurité virtuelle ainsi que les fonctions administratives et de gestion dans un seul et même système transactionnel. Une particularité intéressante et extrêmement utile du système TRANZIX est constituée par la façon dont la protection de la communication ainsi que la sécurité des messages est assurée. Plusieurs aspects entrent en jeux au niveau de la sécurité d'un système transactionnel: la sécurité de la banque en tant qu'émetteur et celle des clients – vendeurs ou acheteurs – jouent toutes les deux un rôle primordial. De plus, la confidentialité des communications entre les intervenants doit aussi être assurée.

Nous définissons le terme ***instrument monétaire*** comme étant un objet physique ou virtuel qui permet de représenter – et souvent de transporter – directement ou indirectement une valeur transigible. Pour servir d'unité d'échange, un instrument monétaire, réel ou virtuel, doit répondre à plusieurs exigences – indispensables à la survie d'un système transactionnel ***généralement accepté***, c'est-à-dire accepté par une proportion significative d'intervenants:

- l'unité monétaire doit être facilement reconnaissable, commode et non dispendieuse à utiliser;
- l'unité monétaire doit être durable, ne pas se détériorer facilement;
- l'unité monétaire doit avoir une valeur relativement stable, offrant une certaine confiance aux intervenants qui l'utilisent. Pour ce faire, l'instrument monétaire peut offrir des indices sur la valeur qu'elle représente, c'est-à-dire, il doit être couvert par d'autres valeurs généralement acceptées (telles que l'or, d'autres devises, des biens ou services, etc.);
- l'unité monétaire doit offrir à l'usager une garantie quant à son authenticité et à l'émetteur une garantie de non-contrefaçon, c'est-à-dire qu'elle doit être difficile à copier.

Ainsi, l'instrument monétaire doit contenir intrinsèquement plusieurs données, organisées dans une structure; nous pouvons donner un sens économique à cette structure à l'aide de conventions. Les systèmes de paiement électronique courants couvrent plus ou moins bien ces aspects. Le fait qu'aucun ne se soit démarqué de façon très nette indique qu'aucun ne remplit complètement toutes ces conditions. Si les trois premières conditions dépendent d'une foule de facteurs externes, la dernière condition dépend de chaque système en particulier.

Attardons-nous sur ce dernier aspect, c'est-à-dire la non-contrefaçon, qui relève de façon intrinsèque de la sécurité de tout système transactionnel. Deux éléments essentiels peuvent être identifiés à cet égard: d'une part l'émetteur doit être capable de détecter une fraude et, d'autre part, il doit être capable d'en identifier l'auteur.

Tout d'abord, pour s'assurer contre la plupart des fraudes, tout comme une grande majorité des systèmes actuels, nous utilisons des moyens cryptographiques. La cryptographie offre les mécanismes de base pour la sécurité et la confidentialité des applications nécessitant le transport d'information sur des réseaux numériques [Abardi et Needham, 1996]. L'utilisation de la cryptographie est intéressante, car elle permet l'implantation d'une solution uniquement logicielle et elle offre un niveau de sécurité très élevé. De cette façon, les coûts d'achat, d'installation et de maintenance sont substantiellement diminués.

La cryptographie à clés publiques (ou asymétriques) est aujourd'hui le moyen le plus efficace pour assurer ce haut niveau de sécurité aux données informatiques [Meyer et Matyas, 1982], [Kaufman et al., 1995], surtout lorsqu'ils circulent sur des réseaux publics de communication [Zimmermann, 1998]. En effet, le problème de la factorisation des grands nombres est connu en mathématique comme un problème difficile à résoudre. À ce jour, la force brute – en essayant toutes les possibilités de combinaison des facteurs d'un nombre – est le moyen le plus direct pour

résoudre ce problème; toutefois, pour des nombres ayant plusieurs centaines de bits en longueur, la force brute requiert un effort de calcul trop important pour être réalisable dans un intervalle de temps raisonnable. Un autre avantage important des systèmes cryptographiques asymétriques est qu'ils permettent d'effectuer des signatures numériques, assurant ainsi l'authenticité et l'intégrité des messages transportés. Par exemple, à l'aide de sa clé privée, la banque peut signer les billets virtuels et certifier les documents électroniques, ce qui est indispensable pour un système électronique de transfert de valeurs. De plus, l'échange de clés peut se faire en toute sécurité en employant le même canal de communication, sans compromettre, d'aucune façon, leur intégrité et leur confidentialité. Un tel système implique une paire de clés numériques qui se complètent par une complémentarité réciproque: un message est encodé avec l'une et décodé avec l'autre. Une des clés, peut être publique, tandis que l'autre, restera secrète. Ainsi, par exemple, la banque va publier sa clé publique, ce qui permettra aux clients d'encoder des messages pour banque, messages qui seront décodés à l'aide de sa clé privée.

L'autre aspect, tout aussi important et indispensable, concerne la confiance dans l'authenticité assurée par le système; non seulement les utilisateurs de ce système doivent avoir un niveau minimal de confiance dans l'authenticité des instruments monétaires – préférablement une très grande confiance –, mais ils doivent aussi être capables de reconnaître et d'authentifier leurs partenaires transactionnels afin de pouvoir avoir confiance dans le bon déroulement de toute transaction. Cette authentification permettra, dans le cas d'une transaction non-réussie, ou qui doit être revue pour toute raison valable, de retrouver toutes les entités transactionnelles afin de résoudre un conflit potentiel[5].

[5] Il existe toutefois une exception à cette règle: une entité peut choisir d'assumer tous les risques en permettant aux autres certains privilèges, comme par exemple, cacher leur identité et leur adresse électronique afin d'effectuer des transactions anonymes.

Pour augmenter la confiance dans la capacité d'authentification du système, nous avons décidé de renforcer les outils cryptographiques employés, par des moyens biométriques. La biométrie est déjà reconnue comme un élément essentiel dans l'authentification de l'identité des usagers et peut sécuriser davantage les infrastructures à clés publiques en assurant des informations claires et complètes sur toutes les entités transactionnelles. La biométrie est aussi considérée comme une technologie qui permet de renforcer la sécurité et la confiance dans les techniques d'authentification et dans les signatures numériques.

Nous avons choisi d'utiliser les signatures manuscrites comme instrument biométrique d'authentification. Pourquoi utiliser les signatures manuscrites ? C'est une des méthodes les moins coûteuses pour effectuer des identifications biométriques, tout en restant efficace, car les signatures manuscrites des clients sont déjà présentes dans les formulaires d'ouverture de compte. Non seulement il est peu coûteux de capter ces signatures manuscrites – un simple numériseur suffit, et ce module matériel n'est requis que pour l'émetteur –, mais leur traitement, une fois prélevées, est rapide et peu encombrant; de plus, il implique des coûts d'utilisation minimes.

Notons aussi que ces données biométriques renforcent la confiance des utilisateurs dans le système: le gouvernement américain, par l'intermédiaire de la **FDA** (*Food and Drug Administration*) mentionne que des moyens biométriques d'identification reliés à une signature électronique lui confèrent une valeur juridique accrue, *égale*[6] à celle des signatures manuscrites déposées sur des documents légaux, rendant cette signature facilement reconnaissable devant une cour de justice.

---

[6] «*[...] electronic signatures that employ at least two distinct identification components such as identification codes and passwords, and electronic signatures based on biometrics are equally acceptable substitutes for traditional handwritten signatures.*» [FDA, 1997]

4.4.3 Sécurisation par moyens cryptographiques

Le système TRANZIX est protégé par des algorithmes très connus, qui ont été déjà testés et mis à l'épreuve, ce qui nous permet de croire qu'ils ne contiennent aucun vice caché. Nous employons un chiffre asymétrique, permettant d'encrypter et de signer, un chiffre symétrique aidant à l'encryptage plus performant des données, et un algorithme de hachage qui aide à assurer l'intégrité des données transmises.

4.4.3.1 La sécurité des communications

Le système que nous proposons emploie le PTEV, qui, à son tour, utilise trois algorithmes cryptographiques comme moyen de sécurisation:

1. ***RSA*** (*Rivest, Shamir, Adleman*) – chiffre asymétrique utilisant des clés à longueur variable;
2. ***IDEA*** (*International Data Encryption Algorithm*) – chiffre symétrique utilisant une clé de longueur fixe de 128 bits;
3. ***MD5*** (*Message Digest 5*) – algorithme contenant une fonction unidirectionnelle servant à «hacher» un message [Tsudik, 1992] pour générer un court résumé binaire de 128 bits.

Regardons de plus près les bases mathématiques de l'algorithme RSA. Tel que spécifié dans [Rivest et al., 1978], cet algorithme utilise des calculs exponentiels et des opérations modulo pour effectuer ses fonctions cryptographiques telles que l'encryptage et le décryptage.

Tout d'abord, deux nombres p et q sont générés, ayant la propriété que les deux sont des nombres premiers et qu'ils sont suffisamment grands (plusieurs centaines de bits). Soit x un message et m le produit $m = p \times q$; alors:

$$x^{(p-1)\times(q-1)} = 1[mod(p \times q)] \tag{4.1}$$

si x n'est pas divisible ni par p ni par q. Pour générer une paire de clés, deux nombres sont choisis arbitrairement, e et d, ayant la propriété que:

$$e \times d = 1[mod((p-1)\times(q-1))] \tag{4.2}$$

e sera alors la clé d'encryptage – partie intégrante de la clé publique –, tandis que d sera la clé de décryptage. ou la clé privée (appelée aussi clé secrète). Ainsi, toute donnée encryptée avec e peut être décryptée avec d:

$$(x^d)^e = x[mod(p \times q)] \tag{4.3}$$

Alors le nombre e, peut être rendu public, ensemble avec le produit $m = p \times q$ (formant ainsi la clé publique), sans toutefois révéler ni p, ni q, ni la clé secrète d. Le principal point fort de l'algorithme repose sur la difficulté de factoriser des nombres aussi grands afin de pouvoir retrouver p, q et d. Toutefois, ceci constitue aussi un désavantage: le temps de calcul est considérable et la puissance de calcul nécessaire pour le diminuer est importante.

Pour réduire le temps de calcul, en sachant que le temps nécessaire pour effectuer des calculs exponentiels RSA n'est pas négligeable, le chiffre symétrique IDEA [Schneier, 1996] sera utilisé pour encrypter le contenu des enveloppes virtuelles (Fig. 4.14), employant une clé unique et aléatoire pour chaque transfert – la ***clé de session***. Cette clé est elle-même transmise au destinataire; avant d'être ajoutée au message transactionnel dans l'enveloppe virtuelle, la clé de session sera encryptée à l'aide de l'algorithme RSA. Ainsi, le message transactionnel sera composé par les données encryptées avec le chiffre IDEA et par la clé de session encryptée avec l'algorithme RSA. Cet artifice permet de réduire de façon substantielle le temps de

calcul, ce qui constitue un élément extrêmement important dans un protocole multi-messages et multi-usagers.

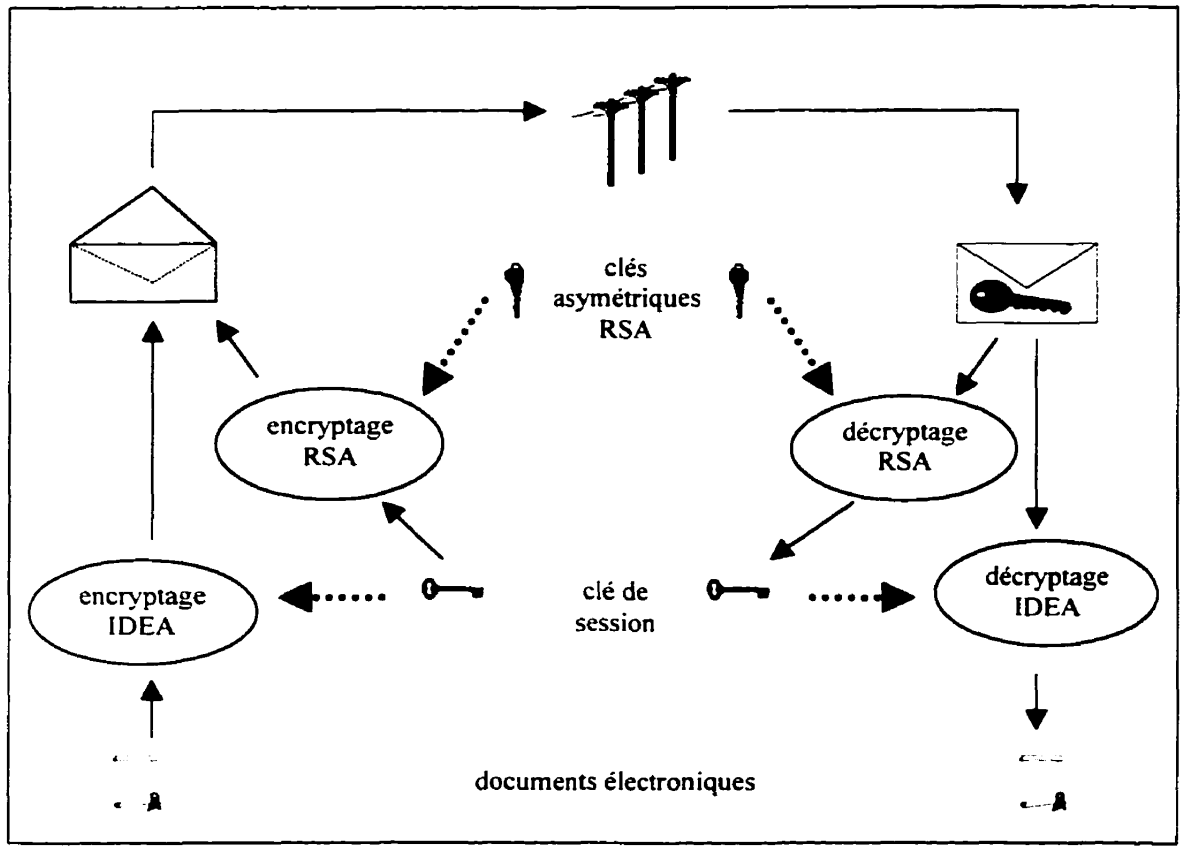

Figure 4.14 – *Le transport et la protection des enveloppes virtuelles*

Notons le fait que le chiffre symétrique IDEA est un chiffre qui opère sur des blocs de données ayant chacun 64 bits de longueur. L'encryptage implique 8 séries d'opérations mathématiques sur 4 sous-blocs de 16 bits, dans chaque bloc de données. Les opérations effectuées entre ces sous-blocs et les sous-clés de 16 bits de la clé d'encryptage sont: *XOR* («ou» logique exclusif), addition modulo 2^{16}, ainsi que la multiplication modulo $(2^{16} + 1)$. La vitesse d'exécution est deux fois supérieure à celle de l'algorithme bien connu DES et la sécurité assurée par IDEA est considérée très bonne [Schneier, 1996].

En ce qui concerne l'intégrité des messages, elle est assurée par des signatures numériques effectuées à l'aide de l'algorithme RSA, incluant un sommaire des données signées. Ce sommaire est recalculé à la destination, un résultat identique indiquant que les données n'ont pas été modifiées en cours de route. L'algorithme MD5 [Schneier, 1996] utilisé pour le calcul du sommaire effectue le hachage du message ou des données à signer en employant des opérations unidirectionnelles basées sur quatre fonctions non-linéaires logiques et une mathématique.

Ainsi, les données d'entrée sont divisées en blocs de 512 bits et les fonctions non-linéaires sont appliquées sur des sous-blocs de 32 bits de chaque bloc. Ces fonctions sont: *OU* («ou» logique), *XOR* («ou» logique exclusif), *ET* («et» logique), *NON* (négation logique) ainsi que $int(2^{32} \times abs(sin()))$ – où *int()* est la fonction qui calcule la valeur entière et *abs()* est la fonction qui calcule la valeur absolue. Les résultats de ces calculs consistent en quatre sous-blocs de 32 bits, concaténés dans un seul bloc de 128 bits, le sommaire final. Notons que ces procédures peuvent être étudiées plus en détail dans des ouvrages spécialisés, tels que [Schneier, 1996].

Afin d'illustrer le fonctionnement interne du moteur cryptographique, regardons comment sont effectuées les principales opérations cryptographiques du système TRANZIX. Soit:

- *X* un billet ou message;
- *P0()*, *P1()* et *S0()*, *S1()* des clés publiques, et privées, respectivement, employées par le chiffre asymétrique RSA; alors *P0(X)* représente le message encrypté avec la clé publique P0(), ayant la particularité que $S0(P0(X)) = X$;
- *k* une clé privée de session employée par le chiffre symétrique IDEA; ainsi, ce chiffre est son propre complément: $IDEA(IDEA(X, k), k) = X$;
- *MD5(X)* une représentation sur 128 bits de *X*.

Alors pour encrypter un billet, message ou document, il faut effectuer un calcul d'encryptage symétrique des données, un calcul d'encryptage asymétrique de la clé de session et une concaténation: *[IDEA(X, k), P1(k)]*, *P1()* étant la clé publique du destinataire. Pour signer un billet, message ou document, il faut effectuer un calcul de hachage des données à signer, un calcul de génération d'une signature numérique sur le résultat du calcul de hachage et une concaténation: *[X, S0(MD5(X))]*.

Pour encrypter et signer un billet, message ou document, il faut effectuer plusieurs calculs cryptographiques et une concaténation: *[IDEA([X, S0(MD5(X))], k), P1(k)]*; pour décrypter un billet, message ou document, il faut effectuer un calcul cryptographique: $X = IDEA(IDEA(X, k), k)$ où $k = S1(P1(k))$, S1() étant la clé sécrète du destinataire. Enfin, pour authentifier un billet, message ou document, il faut effectuer quelques calculs cryptographiques et un test:

SI *MD5(X) = P0(S0(MD5(X)))*
ALORS le billet, le message ou le document est authentique.

Cinq opérations cryptographiques de base sont utilisées dans le système TRANZIX:

1) la génération des clés, procédure par laquelle une paire de clés asymétriques est créée. Cette paire peut être permanente ou avoir une date d'expiration;
2) l'encryptage RSA + IDEA, opération qui génère la clé de session IDEA sur 128 bits, qui encrypte à l'aide de cette clé et du chiffre IDEA les données cibles et qui encrypte la clé de session à l'aide du chiffre RSA avec la clé publique du destinataire;

3) le décryptage RSA + IDEA, opération qui décrypte la clé de session à l'aide de la clé secrète du destinataire et du chiffre RSA, et utilise le résultat pour décrypter les données cibles;
4) la génération des signatures numériques, opération qui emploie la fonction de hachage comme contrôleur d'intégrité pour obtenir un résumé sur 128 bits des données cibles et qui utilise ce résumé, le chiffre RSA et la clé sécrète de l'expéditeur pour générer une signature numérique;
5) la vérification des signatures numériques, procédure qui utilise la fonction de hachage pour obtenir un résumé des données cibles qui est immédiatement comparé avec le résumé signé afin de vérifier leur intégrité, et qui utilise le chiffre RSA et la clé publique de l'expéditeur pour vérifier la validité de la signature.

La sécurité des communications est assurée par l'encryptage des messages TRANZIX (messages informatifs de haut niveau ou enveloppes virtuelles), avec les composantes cryptographiques décrites précédemment. Nous n'avons pas trouvé utile d'encrypter le canal de communication au complet car cela aurait impliqué l'ajout de longues secondes d'attente pour l'encryptage et le décryptage de chaque message de contrôle du protocole transactionnel.

Le protocole de communication n'est donc pas tunnelisé et ce, sans aucune perte de confidentialité ou diminution du niveau de sécurité. Comme le maillon faible de cette approche cryptographique est constitué justement par les longs calculs cryptographiques qui prennent une quantité considérable de temps, l'effet final est amplifié encore plus par la lenteur de l'exécution d'un langage interprété comme Java.

Les messages de contrôle – requêtes/réponses – du protocole transactionnel ne sont donc pas encryptés. Voilà donc un point vers lequel une éventuelle attaque

pourrait être dirigée. La protection que nous avons introduite à ce niveau pour contrer cette éventualité consiste à restreindre très sévèrement le protocole, qui n'accepte aucun message «hors-contexte» ou «hors-séquence»[7]. De plus, même si le protocole ou le canal de communication sont pénétrés, aucune protection additionnelle n'est nécessaire, car le seul élément précieux transporté est l'enveloppe virtuelle TRANZIX qui, elle, est encryptée; il est donc inutile d'«écouter» le canal de communication afin de «voler» le billet et de l'utiliser de façon frauduleuse. Il n'est pas possible non plus d'introduire sur le canal de communication un message erroné ou ayant une signature incorrecte. Dans le premier cas, ce message sera détecté lors de la vérification locale d'intégrité et du décryptage; dans le second, la signature incorrecte sera détectée lors de la vérification locale de l'intégrité. En conclusion, nous n'utilisons pas l'encryptage complet du canal de communication, ce qui conduit à des économies importantes en temps de calcul, sans affaiblir la sécurité du système.

4.4.3.2 La protection des billets virtuels

Nous avons vu dans la section «4.3 Design préliminaire», sous-section «4.3.3 La structure des données», comment sont constituées les enveloppes virtuelles. Nous avons vu que ces enveloppes peuvent transporter n'importe quelle charge binaire et que l'information interne est structurée en trois composantes: l'information utile, l'information de contrôle et le champ de remplissage. Nous avons vu aussi comment l'intégrité de l'information utile est contrôlée par l'information de contrôle et comment le champ de remplissage permet de combattre les méthodes de décryptage utilisant l'analyse du trafic.

---

[7] Un message «hors-contexte» est un message contenant des données sans rapport avec le protocole transactionnel, introduisant des données possiblement corrompues. Un message «hors-séquence» est un message qui pourrait faire partie du protocole transactionnel, mais qui a été inséré au mauvais endroit, ne se trouvant donc pas à la bonne place dans la séquence des messages transactionnels.

À part les documents électroniques pouvant représenter différentes valeurs, le contenu principal des enveloppes virtuelles est constitué par les billets numériques. Ainsi, physiquement, les billets virtuels sont constitués par des fichiers binaires contenant de l'information encryptée stockée à l'intérieur d'une enveloppe virtuelle.

La structure des billets est divisée en plusieurs éléments – ou champs –, de façon à garder un bon compromis entre la sécurité et la compacité nécessaire à l'obtention des bonnes vitesses de transmission. Voici les champs composants de chaque billet virtuel:

- la valeur nominale;
- la granularité
- le nom de la devise;
- le numéro de série;
- la date d'émission;
- la date d'expiration;
- les coordonnées d'identification générale et la signature électronique de la banque émettrice;
- la mémoire active (ou l'historique) contenant des champs biométriques (des pointeurs vers la signature manuscrite d'un ou plusieurs possesseurs [antérieurs] du billet);
- les champs de contrôle;
- le champ de remplissage (servant à prévenir les éventuels essais et de décryptage et d'analyse de trafic).

La Figure 4.15 montre comment ces champs sont distribués. Étant donné que les signatures biométriques subséquentes ajoutées à l'historique du billet s'appliquent au billet au complet, l'entête de chaque nouvelle signature s'ajoute au tout début du billet.

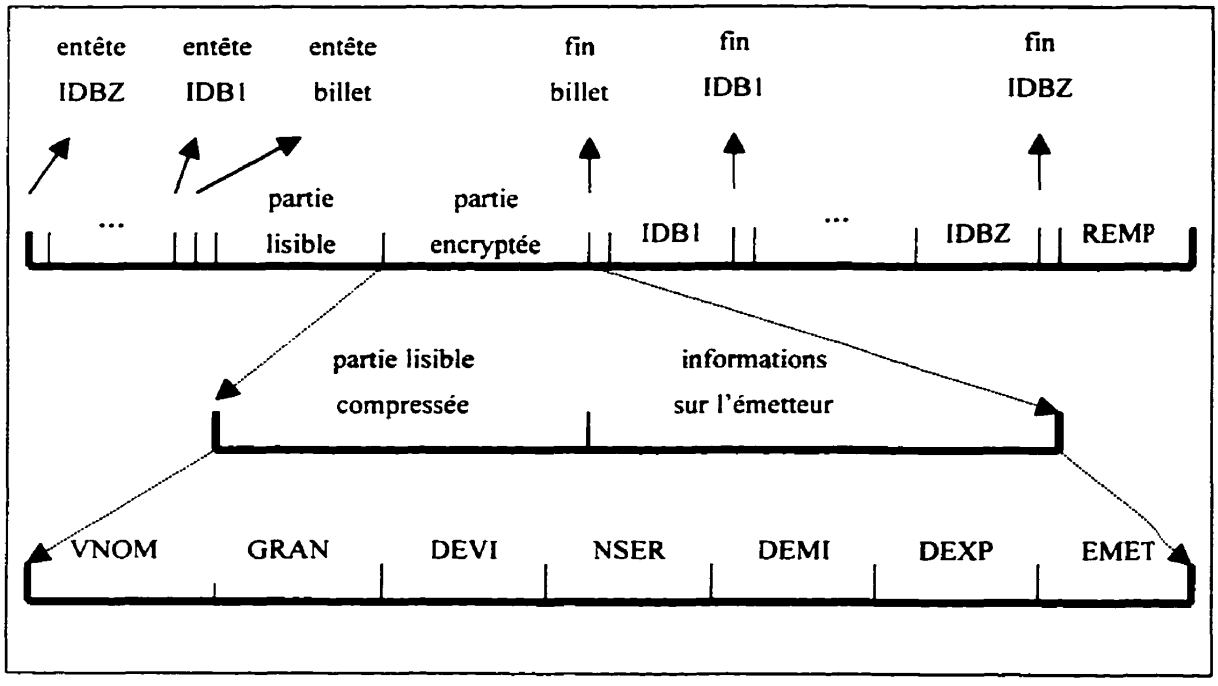

Figure 4.15 – *La structure interne d'un billet virtuel*

Les mnémoniques utilisées dans la Figure 4.15 sont:

- Entête billet: C'est le début du billet; il contient la position, par rapport au début du billet, du début du champ de remplissage, ainsi que sa longueur, en octets;
- Fin billet: la fin du billet contient une vérification de somme (*checksum*) du fichier;
- VNOM = Valeur nominale du billet (par exemple: 0.0001, 1, 10, etc.);
- GRAN = Fraction minimale ou granularité de la devise (par exemple: 0.01, 1, etc.);
- DEVI = Nom de la devise (par exemple: CND, USD, DEM, JPY, etc.);
- NSER = Numéro de série;
- DEMI = Date d'émission;
- DEXP = Date d'expiration;

- EMET = champ qui inclut le nom et les coordonnées de l'émetteur, l'endroit et la version d'émission, le type de couverture[8] de la devise numérique, ainsi que sa signature numérique);
- IDB[1 - Z] = il s'agit de l'ID-biométrique d'un client ayant utilisé le billet – il y a Z places dans l'historique du billet, impliquant le fait que les derniers Z propriétaires du billet sont enregistrés. Chaque champ IDB contient un marqueur d'en-tête et un marqueur de fin qui ne contiennent aucune information sur les signataires; les différents champs IDB encadrent le billet et s'y ajoutent au fur et à mesure que la mémoire active est remplie;
- REMP = Champ de remplissage.

La partie lisible contient tous les champs informatifs du billet en clair (valeur nominale, fraction minimale, devise, numéro de série, dates d'émission et d'expiration, les coordonnées de l'émetteur, la version de l'émission ainsi que le type de couverture de la devise virtuelle). De cette façon, les usagers pourront lire et vérifier visuellement le contenu lisible de chaque billet en cas de besoin. La partie encryptée contient les mêmes informations, mais compressées avec l'utilitaire `GZIP`, encryptées et signées (par l'émetteur et pour l'émetteur) avec IDEA + RSA et encodées avec un utilitaire de type `uunecode` pour pouvoir passer par des passerelles sans erreurs de conversion de caractères.

Regardons comment ces champs sont crées et assemblés pour former un billet virtuel – une des informations fondamentales transportées par le système TRANZIX. L'architecture interne du système prévoit trois phases importantes dans la

[8] Le type de couverture dépend d'un émetteur à un autre. Par exemple la couverture de la devise peut être totale, ou «1 à 1» (*swap* ou *peg*), c'est-à-dire que chaque dollar virtuel est couvert par un dollar réel déposé à la banque émettrice. Cette couverture peut aussi être partielle ou nulle; plus de détails seront présentés dans le Chapitre 6.

préparation et l'émission des billets numériques: la collecte des informations de base, la mise en forme du billet et la préparation de l'enveloppe virtuelle.

Les deux premières phases comportent 6 étapes, tandis que la préparation de l'enveloppe en comporte 4. Afin de voir comment les valeurs contenues dans les champs du billet sont créées, nous allons décrire de façon algorithmique, en pseudo-code, leur calcul.

A. Collecte des informations de base:

1. LET Valeur nominale = valeur à spécifier par l'administrateur qui effectue l'émission;
2. LET Devise = valeur à spécifier par l'administrateur qui effectue l'émission;
3. LET Numéro de série = valeur générée dans le module b-1.11 «Émettre des billets», en partant de 0 et en regardant le dernier numéro émis;
4. LET Date d'émission = lire date/heure à partir de l'horloge interne du serveur de l'entité banque;
5. LET Date d'expiration = valeur à spécifier par l'administrateur qui effectue l'émission (par défaut = Date d'émission + 90 jours);
6. LET Émetteur = valeur à spécifier par l'administrateur en utilisant ses bases de données, notamment la banque des clés.

B. Mise en forme du billet

1. Combiner ensemble les champs VNOM, GRAN, DEVI, NSER, DEMI, DEXP, EMET pour former la partie lisible du billet;
2. Copier, compresser, encrypter et signer numériquement ce résultat;
3. Créer et remplir le champ de remplissage la mémoire active non-utilisée;
4. Créer l'entête du billet, incluant la position et la longueur du champ REMP;
5. Concaténer les champs crées et calculer la vérification de somme (*checksum*) du billet;
6. Créer la fin du billet.

C. Préparation de l'enveloppe virtuelle

1. Ajouter les champs DEST et EXPD;
2. Déterminer et ajouter le champ TYPE;
3. Calculer la vérification de somme (*checksum*) pour le fichier ainsi obtenu;
4. Ajouter les champs de contrôle de début et de fin de fichier.

Il n'est pas difficile de voir que toutes ces étapes de traitement comportent des opérations séquentielles répétitives qui peuvent être effectuées dans un intervalle de temps court. Ceci permet de traiter rapidement une grande quantité de billets ou de messages transactionnels, rendant possible l'utilisation des micropaiements à des coûts raisonnables.

La vérification des billets électroniques est effectuée par le centre de vérification, module spécialisé du logiciel de l'entité banque (b-1.6). Ce module vérifie chaque billet qui vient d'être déposé auprès de la banque ou qui transite par la banque dans le cadre d'un transfert. Cette vérification est effectuée en regardant l'intégrité logique et la validité de chaque champ constituant du billet, en mettant un accent spécial sur le numéro de série. Ce dernier est comparé à une base de données contenant la liste de tous les numéros de série des billets déjà dépensés. Si le numéro de série du billet se trouve dans cette liste, une tentative de fraude par copiage vient d'être détectée. Si, par contre, la signature de la banque – ou un des champs de contrôle – est trouvée non-conforme (l'intégrité ou la validité a été violée), une tentative de fraude par falsification vient d'être détectée.

Nous conférons une mémoire active à chaque billet, mémoire qui sert de protection au système, lui permettant d'offrir aux utilisateurs le choix de transiger hors-ligne. Un billet sans mémoire ne pourra être utilisé que dans les transactions en-ligne. La banque retrouve à partir de la mémoire active du billet en question un ***historique***

contenant les signatures des Z derniers[9] propriétaires; ces signatures sont comparées avec les signatures contenues dans la base de données, signatures auxquelles pointe le numéro de série retrouvé. Lorsqu'une équivalence est trouvée, la banque récupère à l'aide de l'ID-biométrique les coordonnées du fraudeur et peut le poursuivre en justice. Nous introduisons ainsi un autre élément innovateur en offrant à la banque la possibilité de retracer l'histoire hors-ligne du billet à l'aide de sa mémoire active.

Au pire des cas, dans l'éventualité théorique extrêmement rare, pratiquement impossible[10], dans laquelle aucun ID-biométrique n'est retrouvé ou s'il a été falsifié d'une quelconque façon, la banque rejette le billet et supportera la perte. Ceci pourra cependant être changé, étant donnée la modularité du système; ainsi, la banque pourra décider si elle préfère faire assumer la perte par le client qui a effectué le dépôt du billet en question.

Une fois que le nombre Z de signatures qu'un billet peut porter dans sa mémoire active est atteint (la mémoire est remplie), le billet expire automatiquement et il doit être échangé contre un nouveau billet, à la banque. Physiquement, la mémoire active consiste en un champ de Z cadres de longueur fixe (IDB1 + IDB2 + ... + IDBZ),

---

[9] Z est le nombre maximal de propriétaires qui peuvent laisser leurs traces dans la mémoire active est spécifié par l'émetteur. Une attention particulière doit être portée au choix de ce nombre. Ainsi, un Z trop petit rend le système pratiquement en-ligne, lui enlevant ses capacités de transiger hors-ligne; en d'autres termes, sans avoir suffisamment d'espace dans la mémoire active pour les ID-biométriques des clients qui ont transigé hors-ligne, le billet ne peut plus être protégé, ce qui implique la nécessité de le transiger en-ligne afin d'éliminer les risques de fraude par copiage. De plus, le trafic pour renouveler les billets ayant une mémoire qui peut être remplie très vite, augmente. Un Z trop grand donne une «vie hors-ligne» trop longue aux billets, augmentant ainsi les risques de fraude et rendant plus difficiles les éventuels efforts de retrouver un faussaire.

[10] La probabilité d'une telle erreur est, comme nous allons voir dans les sous-sections suivantes, quasiment nulle. Nous avons toutefois préféré prévoir toutes les possibilités afin de bien clarifier le fonctionnement du système.

chaque cadre permettant l'inscription automatique et transparente, par le logiciel du client, de l'ID-biométrique du propriétaire qui vient de faire l'acquisition du billet.

Un autre aspect dangereux, tel que décrit dans la sous-section 4.4.3, pourrait survenir dans le cas où un malfaiteur, à l'intérieur de la banque émettrice, rendrait publiques les clés privées de l'émetteur, permettant ainsi à tout usager d'émettre des billets valides. Les dommages potentiels qui pourraient être engendrés par un tel problème peuvent être limités en instituant une date d'expiration pour chacun des billets. Chaque billet a donc une durée de vie limitée: même si un billet n'a pas été dépensé, tous les billets en circulation expirent périodiquement, pour des raisons de sécurité, afin de protéger la banque émettrice (contre des éventuelles fraudes internes, par exemple).

Une fois le billet expiré, il ne peut plus être dépensé et il doit être déposé à la banque émettrice en échange d'un nouveau billet, ayant le même montant. L'expiration forcée des billets n'est pas une opération trop lourde à gérer, car la vérification de la date d'expiration se fait de façon distribuée, par chaque portefeuille virtuel, et l'échange des billets a lieu de manière transparente pour l'usager, impliquant un simple dépôt à la banque, suivi d'un retrait du même montant.

En conclusion, tous les sous-critères de sécurité sont remplis, faisant de TRANZIX un système avec un très haut niveau de sécurité: les deux algorithmes de chiffrement – RSA et IDEA – offrent une confidentialité totale des transactions communiquées et permettent en même temps de limiter l'accès au système – seules les membres détenant des portefeuilles virtuels TRANZIX et des clés compatibles et reconnues peuvent s'échanger des messages transactionnels. L'intégrité des communications, l'authentification des entités transactionnelles et, en partie, la non-répudiation des transactions est assurée par des signatures numériques effectuées à l'aide du chiffre asymétrique. Un code local d'accès au portefeuille sert à compléter les exigences restantes des sous-critères d'accessibilité et de non-répudiation, comme nous

allons voir dans la sous-section 4.4.4.4. De plus, l'authentification et la non-répudiation des transactions sont renforcées à l'aide d'une technologie biométrique, comme nous allons le voir en détails dans la sous-section suivante.

4.4.4 Personnalisation du système par moyens biométriques

TRANZIX offre une très forte protection, basée sur des algorithmes cryptographiques à clés publiques. Les communications ne peuvent pas être espionnées, car elles sont encryptées de bout en bout; de plus, tout billet est protégé en encryptant l'enveloppe virtuelle qui le contient.

Ce haut niveau de sécurité est complété par une couche de protection supplémentaire, biométrique, basée sur des signatures manuscrites. En protégeant chaque billet virtuel nous nous assurons qu'un seul et unique billet peut porter un numéro de série donné, dans tout le système. En effet, un billet ayant un numéro de série inexistant sera découvert immédiatement comme faux, car il n'aura sûrement pas été signé par la banque. Un billet copié sera détecté dès son dépôt, car même si la signature de la banque est valide, l'émetteur détectera la présence de deux numéros identiques dans sa base de données.

Pour les transactions en-ligne, ce processus d'identification d'un faussaire est immédiat. Le problème se complique lors de l'utilisation des billets dans les transactions hors-ligne, dans lesquelles un billet peut transiter sur les disques durs et les disquettes de plusieurs clients avant de se retrouver à la banque pour être vérifié. C'est aussi à ce niveau qu'intervient un autre élément essentiel pour la sécurité du système: l'identification d'un éventuel fraudeur.

Si pour les transactions en-ligne, comme nous venons de voir, une signature électronique pourrait être suffisante pour empêcher le copiage, il est plus difficile de retrouver le coupable lors d'une transaction hors-ligne. Nous avons décidé d'identifier clairement tous les clients, et ce pour toute transaction, afin de pouvoir identifier hors de tout doute le responsable d'une éventuelle fraude, diminuant ainsi les risques pour chacune des entités transactionnelles et augmentant la confiance des utilisateurs dans le système.

L'identification des clients est réalisée à l'aide de plusieurs types d'information. D'une part nous avons les données personnelles des clients, telles que fournies à l'ouverture d'un compte; d'autre part, nous avons une identification ou une signature biométrique associée à chaque client, afin de conférer un haut niveau de sécurité au système, et renforcer ses capacités d'authentification et de non-répudiation.

La signature manuscrite est le moyen le plus efficace du point de vue sécurité, commodité et prix pour effectuer une identification biométrique et, de plus, elle est reconnue légalement comme preuve d'acceptation d'un contrat ou d'une transaction. Les signatures manuscrites sont des cas particuliers de l'écriture manuscrite, très souvent illisible. Pour cette raison, entre autres, plusieurs systèmes d'analyse et vérification des signatures manuscrites existants [Plamondon et Lorette, 1989], [Leclerc et Plamondon, 1994] traitent ces signatures comme des images [Plamondon et al., 1990]. En s'inspirant de cette idée, TRANZIX utilise à son tour les images des signatures manuscrites des clients pour des fins d'identification et de sécurisation, sans toutefois appliquer des mécanismes de vérification.

Il est donc important de mentionner le fait que notre approche n'implique pas de technique de vérification de signatures manuscrites, car la signature n'est prélevée qu'une seule fois et elle n'est pas comparée avec d'autres spécimens. Une fois prélevée, la signature sert à protéger les clients et leurs fonds en assurant un moyen

efficace pour identifier et poursuivre un éventuel fraudeur. Malheureusement, une signature manuscrite représentée par une image numérique comporte un nombre élevé de pixels, ce qui génère une très grande quantité d'information à transporter de façon courante et répétée sur des réseaux numériques. Ceci peut être problématique, surtout pour les usagers ayant des connexions à basse largeur de bande. Pour atténuer ce problème, nous avons cherché un moyen d'extraire seulement quelques parties du fichier de l'image, afin de diminuer la quantité d'information.

La solution que nous proposons ici implique la création d'un ***numéro biométrique personnel*** permettant d'identifier une personne par sa signature, en condensant dans un espace réduit des informations essentielles et distinctes contenues dans sa signature manuscrite. Le numéro biométrique personnel est représenté physiquement par une chaîne de chiffres corrélés aux informations tirées de l'image d'une signature. Ces informations sont représentées par des niveaux de gris dans une image numérisée d'une signature manuscrite prélevée à partir du formulaire de demande d'ouverture de compte, signé par le client. Pour arriver à cette chaîne, l'image est divisée en plusieurs mèches verticales (ou, de façon optionnelle, diagonales) de largeur variable. Chaque mèche comprend une ou plusieurs lignes horizontales de pixels; la moyenne des intensités de ces pixels est calculée pour chaque ligne horizontale de chaque mèche, formant ainsi une suite de valeurs numériques.

La signature biométrique, désignée aussi comme nous l'avons déjà vu, par le terme ID-biométrique, est représentée par une suite de chiffres formée à partir du numéro biométrique personnel, d'un numéro de série et d'une signature électronique. Comme l'ID-biométrique d'un client est écrit dans l'historique du billet dès sa réception, TRANZIX utilise donc des ***billets numériques personnalisés***. Nous allons regarder de plus près, dans les sous-sections qui suivent, comment le numéro biométrique personnel et l'ID-biométrique sont construits.

4.4.4.1 Le numéro biométrique personnel

La banque évite le problème de la double-dépense des billets, tel que défini dans les sections précédentes, en enregistrant les numéros de série des billets déposés – que ces billets aient été retirés et encaissés ou non. Toutefois, ce procédé n'assure pas une protection totale contre le copiage que pour les transactions en-ligne. Pour les transactions hors-ligne – aspect essentiel de notre système – TRANZIX emploie des procédures de protection supplémentaires. Ainsi, l'authentification – élément essentiel et indispensable pour retrouver un faussaire hors-ligne – est renforcée en utilisant les images des signatures manuscrites des clients, ce qui, de plus, assure aussi un important renforcement de la non-répudiation des transactions.

Regardons comment sont obtenues les informations biométriques. À partir de l'image du formulaire d'ouverture de compte, l'image de la signature manuscrite est découpée et mise à l'échelle pour obtenir un cadre standardisé. Tel que montré dans la Figure 4.16, l'image contenue dans le cadre standardisé est filtrée et divisée en deux parties, afin de former, avec des éléments additionnels, la signature biométrique de chaque usager TRANZIX. Il est à noter qu'aucune segmentation ou analyse n'est appliquée à l'image originale; l'image statique de la signature est pixelisée[11], mais elle peut être optionnellement compressée davantage par d'autres algorithmes de compression.

Tout d'abord, la partie contenant la signature manuscrite du client de l'image numérisée – ayant 256 niveaux de gris, codées sur 8 bits – est découpée et mise à l'échelle, afin de ramener toutes les signatures à des dimensions standards. Évidemment,

---

[11] Nous définissons le terme ***pixelisation*** comme étant l'opération par laquelle une image est filtrée afin de créer une reproduction ayant comme éléments de base des pixels plus grands; l'intensité et la position de chaque nouveau pixel est calculée à partir des pixels de l'image originale par une fonction quelconque.

cette mise à l'échelle introduit un bruit non nul, en plus du bruit de quantification engendré par la numérisation de la signature.

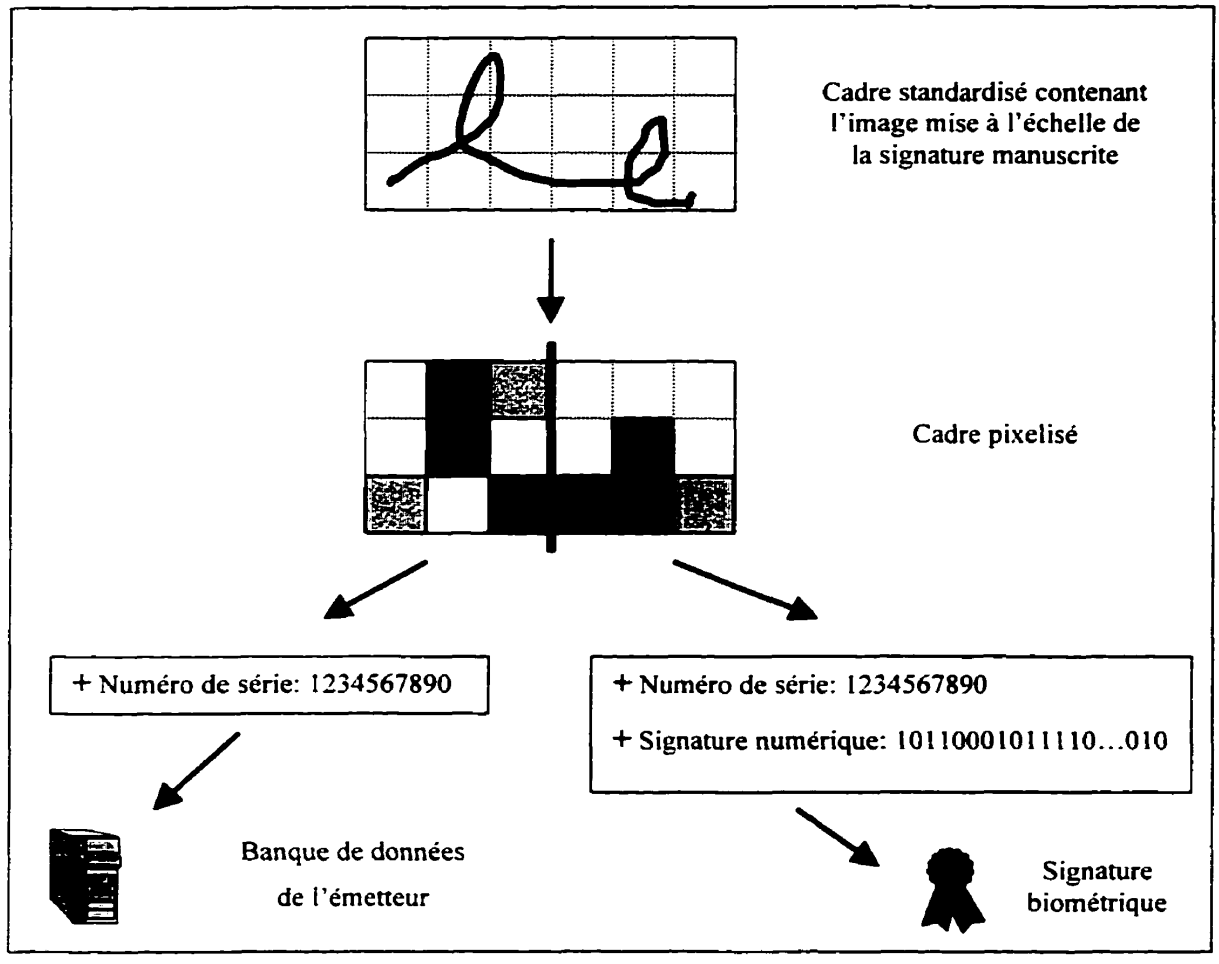

Figure 4.16 – *La création des signatures biométriques*

Concrètement, le cadre standard contenant l'image originale de la signature a une longueur de 256 pixels et une hauteur de 128 pixels. À partir de ce cadre, l'image est filtrée par pixelisation (dans le sous-module b-2.5.2 du DFD), la taille des nouveaux pixels étant choisie arbitrairement lors de la configuration. Évidemment, cette taille aura une influence directe sur la résolution et donc sur la taille de l'image résultante. Le coût d'une bonne résolution résultante est une grande taille de l'image qui engendra alors une

grande taille de l'identificateur biométrique qui circulera sur les réseaux, inclus dans chaque enveloppe virtuelle. Notons que cette opération équivaut à un filtrage qui, à son tour, engendre un bruit causé par la perte de la résolution. L'aspect positif de cette opération est l'effet de compression ainsi obtenu. De cette manière, la suite binaire de l'image pixelisée de la Fig. 4.15, codée sur 2 bits afin de simplifier la lecture, aura la forme:

$$\begin{array}{cccccc} 00 & 10 & 01 & 00 & 00 & 00 \\ 00 & 11 & 00 & 00 & 11 & 00 \\ 01 & 00 & 10 & 10 & 11 & 01 \end{array} \qquad (4.4)$$

Nous pouvons déjà remarquer l'effet de compression obtenu; cependant, notons le fait qu'une pixelisation trop forte pourra engendrer des collisions[12], ce qui implique la nécessité d'augmenter le nombre de bits – noté N, par défaut égal à 8 – sur lequel les niveaux de gris sont représentés et, en même temps, de diminuer la taille des nouveaux pixels, réduisant ainsi le facteur de pixelisation. Un compromis devra donc être effectué entre une optimisation de la taille des signatures biométriques et la résolution des images pixelisées – facteur directement relié au niveau de sécurité.

Les nouveaux pixels sont carrés, tout comme les pixels de l'image originale, ayant les mêmes dimensions sur la verticale que sur l'horizontale. Nous avons choisi un facteur de pixelisation égal à 8 par défaut, soit une taille de 8 pixels de l'image originale pour chaque côté de chaque nouveau pixel de l'image résultante (notons, cependant, que ce facteur est reconfigurable). De cette façon, le numéro biométrique aura: (256 / 8) nouveaux pixels sur l'horizontale, fois (128 / 8) nouveaux pixels sur la verticale, fois 8

[12] Nous définissons le terme ***collision*** pour représenter un conflit crée par la superposition des deux ou plusieurs identificateurs. Ainsi, une collision a lieu lorsque deux images de signatures manuscrites, provenant de deux signataires différents, engendrent un même identificateur biométrique. Le risque de collision est supprimé en ajoutant d'autres informations au numéro biométrique personnel, comme nous allons voir dans la sous-section suivante.

bits pour coder l'intensité de chaque nouveau pixel = 4096 bits ou 512 octets (½ kilo-octets). L'intensité des nouveaux pixels est calculée comme étant la moyenne arithmétique des intensités des pixels qui forment chaque nouveau pixel, comme l'indique l'algorithme suivant, présenté en pseudo-code:

```
LET Pixel_Original [x,y] = l'intensité du pixel courant dans l'image originale
LET Pixel_Nouveau [w,z] = l'intensité résultante du pixel courant dans la nouvelle image
LET Nb_de_pixels_h = la largeur du cadre, en pixels de l'image originale
LET Nb_de_pixels_v = la hauteur du cadre standardisé, en pixels de l'image originale
LET Taille_pixel_nouveau = la taille des nouveaux pixels, en pixels de l'image originale

FOR p_horiz = 0 TO Nb_de_pixels_h STEP Taille_pixel_nouveau DO
    FOR p_vert = 0 TO Nb_de_pixels_v STEP Taille_pixel_nouveau DO
        FOR i = p_horiz TO p_horiz + Taille_pixel_nouveau DO
            FOR j = p_vert TO p_vert + Taille_pixel_nouveau DO
                Pixel_Nouveau [p_horiz,p_vert] += Pixel_Original [i,j];
            END
        END
        Pixel_Nouveau [p_horiz,p_vert] /= (Taille_pixel_nouveau ^ 2);
    END
END
```

L'image résultante contient `(Taille_pixel_nouveau x Taille_pixel_nouveau)` fois moins de pixels que l'original, chaque nouveau pixel ayant une intensité calculée à l'aide de l'équation (4.5):

$$Pixel\_Nouveau(p\_horiz, p\_vert) = \frac{\sum_{i=p\_horiz}^{p\_horiz + Taille\_pixel\_noveau} \sum_{j=p\_vert}^{p\_vert + Taille\_pixel\_noveau} Pixel\_Original(i, j)}{(Taille\_pixel\_nouveau)^2} \quad (4.5)$$

Ce processus de pixelisation engendre évidement une perte de résolution qui augmente le niveau d'ambiguïté de l'image résultante. Afin d'éliminer toute ambiguïté, nous ajoutons, comme nous allons voir dans les pages qui suivent, un numéro de série unique par concaténation et nous renforçons le tout par une signature numérique. L'ID-

biométrique résultant, devient alors un identificateur individuel, pratiquement unique, qui permet de différentier et d'identifier clairement les usagers du système. Afin de diminuer l'augmentation de l'ambiguïté ou pour augmenter l'effet de compression, en fonction du résultat désiré, le facteur N pourrait être augmenté ou diminué, respectivement – pour obtenir éventuellement N_R, le nombre de bits sur lequel les intensités de l'image résultante seront codées[13]. Avec cette nouvelle valeur, l'image résultante sera représentée avec un nombre supérieur ou inférieur de niveaux de gris par rapport à l'image originale. Dans ce cas, l'intensité de chaque pixel original, dans chaque mèche, doit être ajustée en conséquence, afin de la ramener dans le nouvel intervalle de valeurs disponibles. Pour ce faire, l'intensité de chaque pixel sera divisée par $2^{(N-N_R)}$, avant qu'elle soit prise en calcul dans l'équation (4.5) qui devient alors:

$$Pixel\_Nouveau(p\_horiz, p\_vert) = \frac{\sum_{i=p\_horiz}^{p\_horiz + Taille\_pixel\_nouveau} \sum_{j=p\_vert}^{p\_vert + Taille\_pixel\_nouveau} \frac{Pixel\_Original(i, j)}{2^{(N-N_R)}}}{(Taille\_pixel\_nouveau)^2} \quad (4.6)$$

Les mèches formées par les nouveaux pixels peuvent avoir un angle différent de l'angle par défaut de 90° avec l'horizontale. Une inclinaison fixe peut être conférée de façon facultative aux nouveaux pixels afin de maximiser leur densité informationnelle. De cette façon, des mèches diagonales sont obtenues, ayant un angle d'inclinaison t. Cette inclinaison sera ainsi conférée au nouveau cadre complet – et donc à tous les nouveaux pixels qui sont contenus dans ce cadre – et peut être déterminée par l'angle entre la base du cadre et l'inclinaison moyenne de la signature manuscrite (Fig. 4.17). En calculant le gradient de la luminance à l'aide de l'opérateur Sobel [Pratt, 1978], pour une surface contenant les premiers `(Taille_pixel_nouveau x Nb_de_pixels_v)` pixels de l'image, une première indication sur la direction [d'une première partie] du tracé de la signature pourrait être obtenue. Cette direction détermine l'angle t de l'orientation des mèches. Notons que les pixels qui «débordent» le cadre incliné sont

[13] Notons que dans notre système, par défaut, $N_R = N = 8$ bits.

translatés à l'extrémité opposée, c'est-à-dire, ils sont pris en calcul pour la moyenne du nouveau pixel qui se trouve de l'autre côté du cadre standardisé.

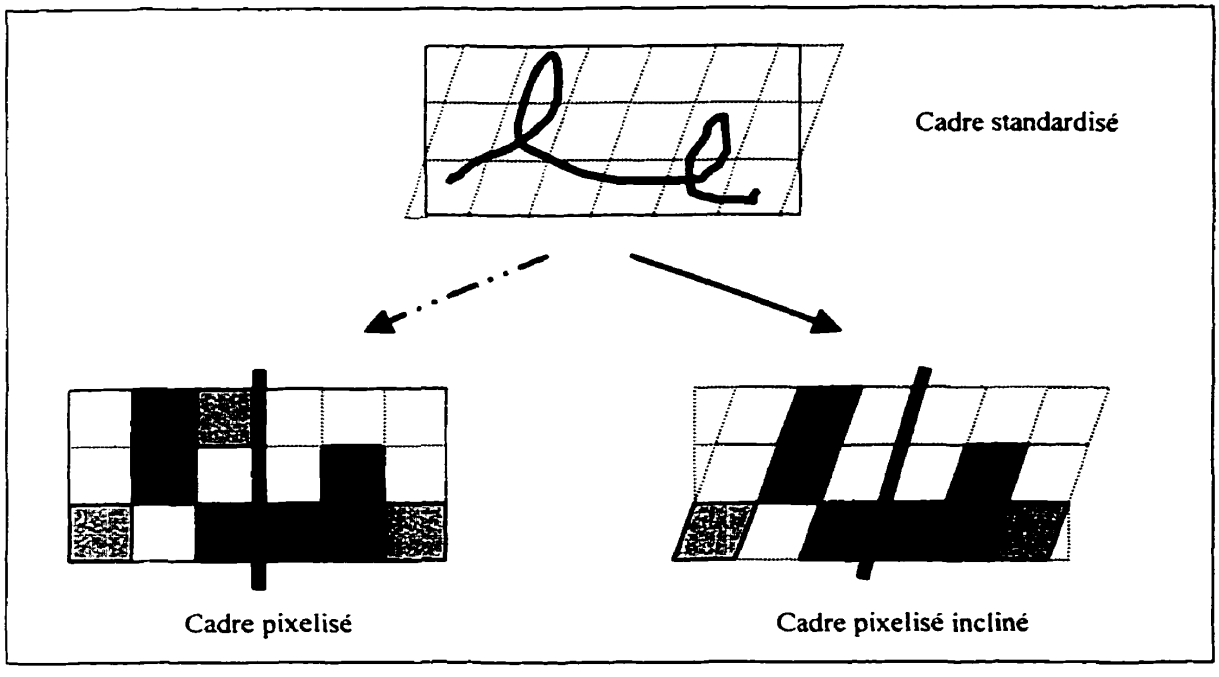

Figure 4.17 – *Cadre incliné*

Le résultat de la pixelisation inclinée aura cette fois-ci la forme suivante:

$$\begin{matrix} 00 & 11 & 00 & 00 & 00 & 00 \\ 00 & 11 & 00 & 00 & 11 & 00 \\ 01 & 00 & 10 & 10 & 11 & 01 \end{matrix} \qquad (4.7)$$

Nous pouvons facilement remarquer la différence entre le nouveau résultat et le résultat initial. Tant dans la Fig. 4.17 que dans la représentation binaire (4.7), l'inclinaison des pixels a permis de réduire le nombre de nouveaux pixels non-nuls et d'augmenter le contraste résultant. Notons qu'il s'agit ici d'un simple exemple; en général, la réduction du nombre de pixels non-nuls et l'augmentation du contraste à

l'aide de l'inclinaison des mèches dépend directement de la forme de la signature manuscrite. En effet, cette procédure est efficace lorsque l'inclinaison de la signature est consistante pour tous ses éléments – la plupart des lettres ou des signes formant la signature ont une inclinaison semblable, en termes de direction et de grandeur de l'angle t. Dans le cas contraire, une inclinaison arbitraire du cadre pourrait avoir un effet inverse à celui désiré, pouvant même augmenter la possibilité de collision. Mais comment éviter une collision des ID-biométriques, générée lorsque deux signatures manuscrites légèrement différentes appartenant à deux signataires distincts – à cause d'une trop basse résolution de l'image filtrée – engendrent un même numéro biométrique ?

4.4.4.2 L'évitement des collisions des numéros biométriques personnels

Comme l'acquisition des signatures manuscrites n'est pas effectuée à l'aide d'une tablette à numériser, mais plutôt à l'aide d'un numériseur d'image, à partir d'une demande d'ouverture de compte sur papier, nous ne pouvons pas effectuer en-ligne l'extraction de certaines caractéristiques dynamiques intrinsèques d'une signature manuscrite, telles que la vitesse, l'accélération ou la pression du trait. Une combinaison de telles caractéristiques permettent d'identifier de façon unique chaque signature, non seulement celles provenant des deux signataires différents, mais aussi celles venant d'un même signataire [Plamondon, 1994]. Par contre, en n'employant qu'un seul spécimen d'une signature manuscrite donnée et sans recourir à des moyens de reconnaissance et de vérification de signatures, nous évitons les problèmes de distorsion, de variabilité ou d'inconsistance des signatures, rencontrés habituellement.

Étant donné que seulement quelques caractéristiques intrinsèques d'une signature manuscrite sont utilisées dans le filtrage par pixelisation, notamment ses dimensions et l'intensité des pixels qui composent son image numérique, et tenant compte de l'existence du bruit introduit par des différentes sources, une collision pourrait être engendrée, surtout lorsque deux signatures manuscrites, provenant de deux

signataires différents, se ressemblent. Notons le fait que la quantité totale de bruit introduite dans le système est un élément difficilement quantifiable et varie fortement d'une signature à une autre, dépendant, entre autres, de la qualité du papier, de la numérisation, etc. De plus, il est difficile à estimer un «facteur de ressemblance» entre deux signatures qui ne sont pas des imitations. Pour de telles raisons, comme nous allons le voir dans les paragraphes qui suivent, le numéro biométrique constitue un élément nécessaire mais partiellement suffisant pour identifier et départager deux individus avec une probabilité d'erreur suffisamment proche de zéro.

Ainsi, nous estimons qu'il y aura une collision si la moyenne des intensités des pixels originaux contenus dans chaque nouveau pixel est égale dans les deux images des deux signatures qui se ressemblent et si la différence entre les coordonnées des pixels originaux formant les traits des deux signatures dans les deux cadres standardisés est plus petite que la taille d'un nouveau pixel, tant sur l'horizontale que sur la verticale. Nous avons vu que la pixelisation entraîne une perte de l'ordre de `(Taille_pixel_nouveau x Taille_pixel_nouveau)` de la résolution. Un effet semblable est obtenu en diminuant le nombre de niveaux de gris, c'est-à-dire en réduisant N. Pour des images binaires, ayant seulement deux niveaux de gris (donc $N = 1$), seule la position des pixels permet de distinguer deux images. Par contre, même si deux pixels se trouvent, dans les deux images cadre, à la même position, à l'aide de plusieurs niveaux de gris ils peuvent toujours être distingués. Statistiquement parlant, après le processus de pixelisation nous aurons dans l'image résultante:

$$N^{\frac{Nb\_pixels\_h}{Taille\_pixel\_nouveau} \times \frac{Nb\_pixels\_v}{Taille\_pixel\_nouveau}} \tag{4.8}$$

possibilités différentes d'avoir une image numérique. Si B représente le bruit total, exprimé en pourcentage des pixels bruités dans le cadre standardisé, ce nombre est

diminué par le facteur de bruit. Ceci implique une probabilité mathématique de l'ordre de:

$$\frac{1}{N^{(1-B)\times\frac{Nb\_pixels\_h}{Taille\_pixel\_nouveau}\times\frac{Nb\_pixels\_v}{Taille\_pixel\_nouveau}}} \tag{4.9}$$

d'avoir deux images identiques. Même si un large pourcentage des pixels n'est pas utilisé, la probabilité exprimée par l'équation (4.9) reste à peu près du même ordre de grandeur. Toutefois, il serait trompeur de croire que toutes ces possibilités sont effectivement utilisables – il est difficile à concevoir, par exemple, une signature composée d'un seul pixel, dans le coin haut-gauche... Nous estimons qu'une proportion significative des signatures sont effectuées en suivant des directions privilégiées, ayant la plus grande densité de pixels près d'une ligne médiane horizontale.

Un autre problème potentiel du numéro biométrique est relié à son intégrité. En effet, le numéro biométrique personnel pourrait être altéré, falsifié ou remplacé par un autre. Pour lui assurer un haut niveau d'intégrité, le numéro biométrique personnel doit alors être signé numériquement, ce qui vient résoudre aussi le problème d'évitement des collisions. Ceci confère l'assurance d'un haut degré de sécurité à des coûts marginaux quasiment nuls. En effet, en ajoutant des signatures numériques le risque de collision est diminué substantiellement pour atteindre une magnitude de l'ordre de 2^{-64} – la probabilité avec laquelle deux messages différents génèrent un même résumé[14] sur 128 bits en utilisant l'algorithme MD5, facteur qui est le double de la probabilité de trouver, par force brute, un message qui engendre un résumé donné (donc le double de 2^{-128}), permettant ainsi de falsifier une signature numérique.

[14] Ainsi, un ordinateur capable de générer un million de tels résumés par seconde, aura besoin d'environ 600,000 ans pour trouver deux messages qui engendrent un même résumé [Schneier, 1996].

En ajoutant donc d'autres données, telles qu'une signature numérique, nous réduisons quasiment à zéro le risque de collision et, du même coup, nous assurons un niveau élevé d'intégrité au numéro biométrique. Si un émetteur utilisant ce système décide de diminuer davantage la probabilité de collision, il n'a qu'a accroître la grandeur du cadre, augmentant ainsi le nombre de pixels ou de réduire le facteur de pixelisation.

4.4.4.3 L'ID-biométrique

Une fois le processus de pixelisation fini, l'image résultante est divisée en deux parties. Une première partie permet de former l'ID-biométrique de l'usager; elle sert ainsi de preuve additionnelle d'authenticité aux entités transactionnelles. L'autre moitié est utilisée par l'émetteur (la banque) pour identifier les éventuels faussaires. Cette division est réalisée en créant deux matrices binaires, contenant chacune une moitié de l'image pixelisée et ayant le format:

$$\left[\frac{Nb\_pixels\_h}{2 \times Taille\_pixel\_nouveau} \times \frac{Nb\_pixels\_v}{Taille\_pixel\_nouveau}\right] \tag{4.10}$$

Concrètement, le numéro biométrique personnel aura deux sous-composantes: la première est une concaténation binaire des lignes contenues dans la première matrice – contenant la première moitié de l'image pixelisée. Cette sous-composante sera incluse dans l'ID-biométrique du client, devenant ainsi partie intégrante de sa signature biométrique. Son ID-biométrique sera ainsi composé par les champs suivants:

- un champ de contrôle;
- un numéro de série (servant aussi comme numéro d'identification du client);

- la signature numérique de l'usager;
- la signature numérique de l'émetteur;
- la sous-composante numéro 1 du numéro biométrique personnel.

La banque gardera la deuxième sous-composante, formée par concaténation binaire des lignes contenues dans la deuxième matrice – contenant la deuxième moitié de l'image pixelisée. Elle gardera aussi la clé publique de l'usager, afin de pouvoir vérifier ses signatures numériques et de pouvoir lui envoyer des messages transactionnels encryptés. La banque gardera dans sa banque de données le complément de l'ID-biométrique de l'usager, formé par les champs suivants:

- un champ de contrôle;
- un numéro de série;
- la signature numérique du client
- la signature numérique de la banque;
- la clé publique du client;
- la sous-composante numéro 2 du numéro biométrique personnel.

De cette manière, en ajoutant ces champs à chaque sous-composante du numéro biométrique personnel, nous pouvons éliminer pratiquement de façon quasi complète tout risque de collision. Cet identificateur devient alors un instrument d'authentification fort, pratiquement infalsifiable, qui pourrait être reconnu légalement dans plusieurs pays, ayant la signature manuscrite des usagers – en plus de la signature numérique – incluse indirectement dans tout message transactionnel futur; à notre avis, plus ce lien biométrique est clair et infalsifiable, plus ce type d'authentification a des chances d'être reconnu et accepté légalement à large échelle. Notons aussi que les calculs effectués pour la génération d'un ID-biométrique sont uniques et ne seront plus répétés, ce qui implique un coût marginal nul par transaction.

La reconstruction de la matrice originale, en mettant ensemble les deux moitiés pour effectuer une identification est réalisée lorsqu'un billet a été dépensé plus qu'une fois ou lorsqu'il a été falsifié. La banque compare les numéros de série des billets déjà dépensés, se trouvant dans sa base de données, avec le numéro de série du billet vérifié; si le billet a été déjà déposé, son numéro se trouve déjà dans la base de données des billets dépensés[15]. La banque peut aussi trouver un faux billet en vérifiant son intégrité – l'intégré des champs ainsi que l'intégrité numérique calculée à l'aide des fonctions de hachage et comparée aux résultats signés de la même opération, effectuée avant la transaction.

Une fois qu'un document électronique ou un billet virtuel a été détecté comme étant faux, la banque extrait l'identificateur biométrique à partir des données en question et peut ainsi reconstruire[16] la matrice originale de l'image pixelisée. Pour ce faire, la banque met ensemble les deux moitiés d'image – une provenant de l'ID-biométrique se trouvant dans l'enveloppe virtuelle du document ou billet en question, l'autre provenant de sa base de données et retrouvée à l'aide du numéro de série unique. À l'aide de ces données dans sa possession, l'émetteur peut ainsi pointer vers les

---

[15] Notons que les billets dépensés sont marqués dans une liste spéciale (Liste des billets invalides, Fig. 4.6). Chaque élément de cette liste contient deux cases: la première contient le numéro d'ordre de la case, qui est le numéro de série d'un billet émis; l'autre contient un fanion indiquant la validité du billet. D'autres cases peuvent être ajoutées optionnellement pour garder d'autres informations. De cette manière, la vérification en-ligne de la présence d'un numéro de série donné sur cette liste ne prend qu'un temps constant, très court.

[16] Comme la pixelisation entraîne une perte de résolution, la reconstruction n'est pas parfaite; il s'agit plutôt de la reconstruction de l'image pixelisée, non pas de l'image originale de la signature manuscrite. Pour avoir un résultat très proche de l'original, il suffit de diminuer le facteur de pixelisation; de plus, même une reconstruction imparfaite est défendable en cour, car elle est accompagnée d'autres informations uniques incluant une signature numérique.

coordonnées du faussaire[17] et le poursuivre en justice – et ceci, avec toutes les preuves dont l'émetteur a besoin pour démontrer la culpabilité du fraudeur. C'est ici que l'avantage d'utiliser des signatures manuscrites se fait sentir: en utilisant un identificateur biométrique reconnu légalement, la responsabilité de chaque entité transactionnelle peut être clairement établie et défendue [ou contestée] en cour.

Ce système de division de l'image permet en même temps d'assurer les usagers contre d'éventuels abus de la part de l'émetteur – qu'il soit une banque ou non. En effet, en ne gardant qu'une moitié de l'image, l'émetteur ne pourra pas reconstituer la signature biométrique complète, car même s'il dispose de la signature sur papier, il ne dispose pas de la clé privée du client et il ne pourra pas changer la date d'émission de l'ID-biométrique, signée numériquement par les deux entités. Pour les mêmes raisons, il ne peut pas non plus utiliser une autre moitié, soit provenant d'une autre image, soit provenant de la même image mais prise à partir d'un autre message, non-falsifié. Ainsi, pour accuser un usager, l'émetteur a besoin non seulement de ses coordonnées et de l'image de sa signature, mais aussi de la date, de l'heure ainsi que d'une copie du message transactionnel signé numériquement par l'usager. La puissance des méthodes cryptographiques employés empêche toute tentative de contrefaçon des signatures numériques, assurant ainsi une très forte protection contre d'éventuelles tentatives de fausse-accusation de la part de l'émetteur.

De cette façon, cet instrument permet à TRANZIX non seulement d'assurer un très haut niveau d'authentification des utilisateurs, mais aussi, à l'aide d'éléments

[17] Notons que, dans certains cas (lorsque, par exemple, l'usager laisse «ouvert», sans surveillance, son portefeuille virtuel), il peut s'agir d'une autre personne que celle à laquelle le compte – et donc la signature biométrique et les coordonnées – appartient. Toutefois, c'est sa responsabilité de protéger son propre portefeuille; cependant, la banque émettrice pourrait décider de limiter les pertes des clients en cas de vol du portefeuille, comme c'est le cas présentement pour les cartes de crédit. Dans un tel cas, les billets retirés directement de la banque pourront être remplacés, mais le compte sera fermé et un nouveau compte, avec de nouvelles clés, doit être ouvert.

complémentaires de sécurité, d'assurer la non-répudiation des transactions. Ces éléments de sécurité – qui complètent les identificateurs biométriques – servent à protéger l'accès au portefeuille virtuel et sont, à leur tour, personnalisables. C'est justement ce que nous allons regarder dans la sous-section suivante.

4.4.4.4 Contrôle de l'accès au portefeuille virtuel

Un aspect très important dans tout système transactionnel est sa capacité d'interdire la répudiation des transactions. Nous avons vu comment, à l'aide des signatures biométriques, TRANZIX offre un bon niveau de non-répudiation. Mais que se passe-t-il si un usager non-autorisé utilise le portefeuille virtuel de quelqu'un d'autre ? Comment savoir si c'est vraiment le bon usager qui effectue les transactions ?

La plupart des systèmes actuels n'offrent aucune protection à ce niveau. Toute personne ayant accès à l'ordinateur du client peut accéder aussi à son portefeuille et effectuer des transactions en son nom. Même si une telle option peut être utilisée dans notre système, nous avons jugé cette alternative comme étant inadéquate. L'approche que nous avons prise consiste plutôt à donner aux usagers des moyens de s'assurer que seul le propriétaire légal d'un portefeuille peut y avoir accès. Ainsi, avant d'effectuer une transaction, l'usager doit «ouvrir» son portefeuille virtuel, qui, par défaut est fermé – les fichiers contenant ses clés, ses billets, et autres informations étant encryptés; une fois «ouvert», le portefeuille reste dans cet état tant que l'usager effectue des transactions locales ou sur le réseau; le portefeuille pourrait se refermer après une période d'inactivité, par exemple deux minutes (paramètre reconfigurable par l'usager).

Concrètement, la protection du portefeuille sera assurée par un mot de passe[18] choisi par l'usager lors de l'installation. Nous avons jugé cette option, qui ne

[18] Même si ce moyen de protection est facilement transmissible, nous l'avons jugé suffisant pour le niveau de sécurité requis pour la phase actuelle de développement du système TRANZIX.

requiert aucun module matériel, comme étant un bon compromis entre la sécurité et la facilité d'utilisation. Le mot de passe est sauvegardé localement et copié de façon sécuritaire dans son compte à la banque, afin de pouvoir le retrouver s'il est perdu ou oublié par l'usager. Le module de protection d'accès au portefeuille est aussi reconfigurable, chaque émetteur pouvant établir ses propres droits et restrictions d'accès pour leurs clients respectifs. En protégeant ainsi l'accès au portefeuille, le client est assuré d'être le seul à pouvoir y accéder, à moins qu'il donne volontairement accès à d'autres personnes; d'une part, le client est protégé lorsqu'il quitte son ordinateur temporairement, et d'autre part, la banque est assurée que la responsabilité d'un message transactionnel appartient à la personne qui détient l'ID-biométrique et le compte respectif. De cette façon, l'usager est à l'abri des accès non-autorisés à son portefeuille virtuel et en signant chaque transaction il ne pourra nier le fait de l'avoir effectué.

Évidemment, d'autres moyens de protection peuvent être utilisés, en fonction du niveau de protection désiré. Ainsi, si un mot de passe est considéré insuffisant pour le niveau de sécurité requis par une application en particulier, l'émetteur peut décider d'utiliser des mécanismes plus complexes, allant jusqu'à l'utilisation des empreintes digitales ou des signatures manuscrites traitées en-ligne par un système de vérification de signatures [Plamondon, 1994]. Dans un tel cas, tous les usagers devront être munis des modules matériels requis pour la lecture des empreintes ou des signatures, respectivement.

4.4.5 Autres moyens de personnalisation

Si la méthode de personnalisation que nous avons décrite dans les sous-sections précédentes – utilisant les images des signatures manuscrites des usagers – n'est pas jugée appropriée ou suffisante pour une application particulière, plusieurs

autres options sont disponibles. La grande flexibilité du système permet d'interchanger arbitrairement des modules différents, ce qui laisse la porte ouverte aux autres types de personnalisation et particulièrement aux autres technologies biométriques.

4.4.5.1 Une approche multi-résolution

Une approche alternative consiste à utiliser des ***ondelettes***. Les ondelettes sont une représentation multi-résolution orthogonale, calculée à l'aide d'un algorithme pyramidal. L'image de la signature manuscrite peut ainsi être réorganisée en une séquence de détails ayant une résolution croissante. À différentes résolutions, les détails d'une image caractérisent généralement des structures différentes du contenu. Ainsi, à basses résolutions, ces détails correspondent au «contexte général» de l'image, mais plus la résolution augmente, plus les détails contiennent des informations précises sur le contenu de l'image. Le grand avantage de cette méthode réside en sa capacité de départager ces résolutions en représentations indépendantes. Étant donnée la séquence de résolutions croissantes $(r_j)_{j\in\mathbb{Z}}$, les détails d'une image à la résolution r_j sont définis comme étant la différence d'information entre l'approximation de l'image à cette résolution et l'approximation de l'image à la résolution plus basse r_{j-1} [Mallat, 1986].

Un ensemble d'ondelettes est employé pour «approximer» une image, chaque ondelette étant construite à partir d'une onde initiale, appelée ondelette mère. Chaque élément de l'ensemble est ainsi une mise à l'échelle (par dilatation ou par compression) accompagnée par une translation de l'ondelette mère. La décomposition de l'image peut se faire en appliquant des filtres multi-résolution passe-bas et passe-haut horizontaux et verticaux, respectivement (Fig. 4.18). L'algorithme pyramidal emploie des convolutions unidimensionnelles des lignes et des colonnes de l'image statique originale avec les filtres multi-résolution. Premièrement les lignes de l'image sont balayées et convoluées avec les filtres multi-résolution horizontaux, en employant la transformation ondelette. Seulement une ligne sur deux est conservée (indiqué par

l'opération ↓2 dans la Figure 4.18) avant de commencer le balayage des colonnes – le restant des lignes étant écarté. Par la suite, chaque colonne est convoluée avec les filtres multi-résolution verticaux, en employant la transformation ondelette – décrite dans l'équation (4.11) de la page suivante; seulement une colonne sur deux est gardée encore une fois, en écartant les autres colonnes. La compression obtenue ainsi n'est pas sans pertes, mais la reconstruction aura, théoriquement, une qualité acceptable.

De cette façon, des sous-images de l'image originale sont obtenues (SI1, SI2, SI3, SI4 dans la Figure 4.18). Le processus peut continuer ainsi, afin d'obtenir le nombre de niveaux de résolution désiré.

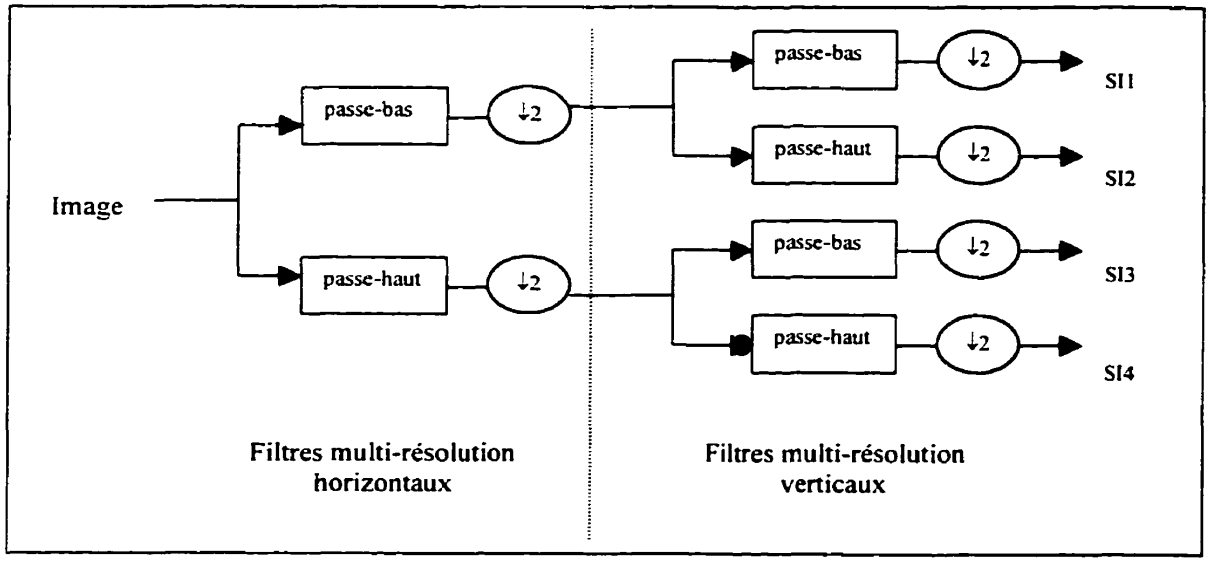

Figure 4.18 – *Décomposition multi-résolution d'une image*

La reconstruction de l'image se fait en sens inverse: entre chaque colonne des sous-images, une colonne de zéros (pixels blancs) est ajoutée avant de convoluer les lignes des sous-images avec les filtres inversés – la transformation ondelette inverse, décrite par l'équation (4.12); une ligne de zéros est ensuite ajoutée entre chaque ligne de l'image résultante, avant de la convoluer avec les filtres inversés.

Regardons de plus près cette transformation. Soit $f(x)$ la fonction représentant le tracé de la signature manuscrite dans l'image statique. L'opérateur de la transformation ondelette est W_g, alors la transformée de la fonction f, par rapport à une ondelette mère g, est définie comme étant:

$$W_g[f(x)](a,b) = |a|^{-\frac{1}{2}} \int f(x) g^* \left(\frac{x-b}{a} \right) dx = W_g f(a,b) \tag{4.11}$$

où $g(x) = e^{jx}$, a est le coefficient d'échelle, b est le coefficient de translation et «*» dénote la conjuguée complexe d'une fonction [Young, 1991]. La fonction assurant la transformation inverse est définie comme étant:

$$f(x) = \frac{1}{c_g} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_g f(a,b) \frac{1}{\sqrt{a}} g\left(\frac{x-b}{a} \right) \frac{dbda}{a^2} \tag{4.12}$$

où:

$$c_g = \int_{-\infty}^{\infty} \frac{|G(\omega)|}{|\omega|} d\omega \tag{4.13}$$

$G(\omega)$ étant la transformée de Fourrier de g.

La Figure 4.19 montre la structure de la transformation directe. En effectuant des produits internes (l'opération I dans la Figure 4.19), tels que décrit dans l'équation (4.14), entre la fonction $f(x)$ et des répliques mises à l'échelle, translatées et conjuguées de l'ondelette mère, les coefficients $W_g f$ sont obtenus, dans le domaine de l'ondelette. Le calcul de ces coefficients est l'essence même de la transformation ondelette.

$$\langle g(x), f(x) \rangle = \int_{-\infty}^{\infty} g(x) f(x) dx \tag{4.14}$$

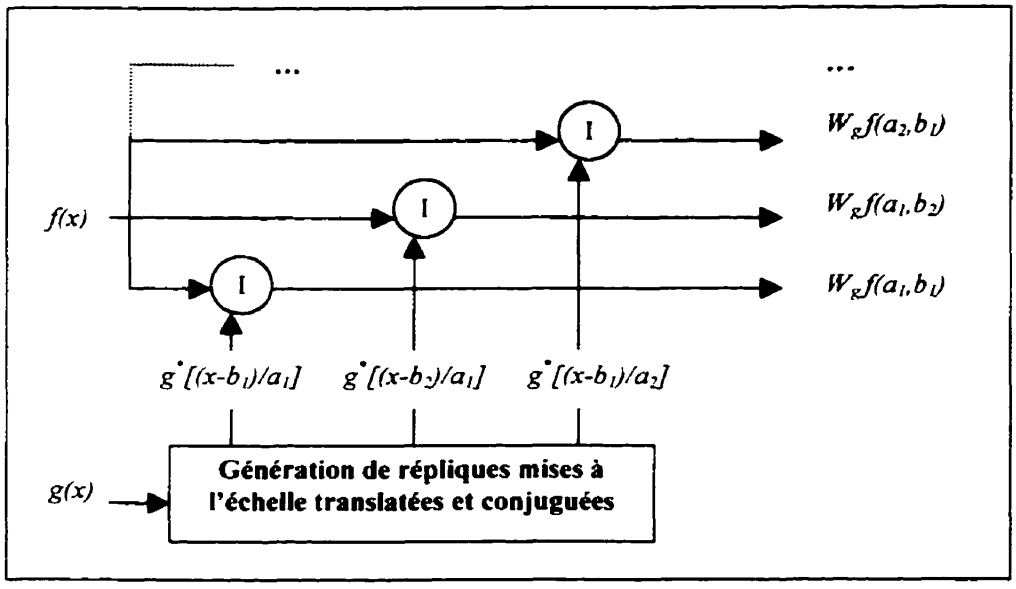

Figure 4.19 – *Structure de la transformation directe*

La transformation directe est utilisée lors de la convolution avec l'image originale pour obtenir ses sous-images et avec les sous-images pour continuer le processus, afin d'obtenir le nombre désiré de niveaux de résolution. La transformée inverse est utilisée lorsque l'image originale doit être recrée.

En appliquant cette transformation à l'image statique de la signature manuscrite, nous pouvons obtenir une représentation multi-résolution ayant n niveaux distincts de résolution. Parmi ces n niveaux de résolution, seulement k niveaux seront utilisés pour former la signature biométrique – n et k choisis en fonction du niveau de sécurité, de la puissance de calcul et de la largeur de bande désirée. Les $(n - k)$ niveaux de résolution – parmi les plus bas – qui restent seront gardés dans la base de données de la banque.

Tout seul, l'émetteur ne peut reconstruire l'image originale car il ne détient que les $(n - k)$ niveaux le plus bas de résolution, sans les détails de l'image se trouvant

dans le k niveaux restants. Il ne peut pas non plus réutiliser la signature du client sur la demande d'ouverture de compte et appliquer de nouveau la transformation ondelette car il ne possède pas la clé privée du client, ce qui l'empêche de falsifier sa signature numérique.

En ce qui concerne la vérification des billets, une fois qu'un faux billet a été détecté, la banque extrait le numéro biométrique du billet et retrouve les autres niveaux de résolution à l'aide du numéro de série. En combinant tous les niveaux ensemble, l'émetteur peut reconstruire l'image originale – avec des pertes[19], toutefois – de la signature manuscrite et retrouver les coordonnées du faussaire. Notons pour conclure sur ce point que cette approche n'est qu'une suggestion théorique d'alternative à la méthode employant la pixelisation et qu'elle ne serait pas implantée par défaut dans TRANZIX.

4.4.5.2 Autres alternatives basées sur les signatures manuscrites

Une autre méthode pouvant être utilisée comme alternative consiste à prendre un nombre prédéterminé de points d'une image de signature manuscrite – par exemple 1024 pixels situés dans 1024 endroits différents mais spécifiés d'avance, dans une structure semblable à un masque statistique uniforme – et de former une chaîne biométrique en concaténant les valeurs de la luminosité de ces pixels ayant des positions prédéterminées. L'avantage d'utiliser un tel gabarit est constitué par sa simplicité qui permet un très grande vitesse de calcul. Un plus grand nombre de pixels, repartis suivant une distribution statistique uniforme concentrée sur l'axe médian de l'image, permet de réduire les risques de collision.

---

[19] Comme celles-ci peuvent être négligeables, la signature manuscrite peut être utilisée comme preuve additionnelle d'authenticité. C'est ici que l'avantage de la réversibilité des transformations effectuées sur l'image de la signature sort en évidence; en effet, plus une image reconstruite ressemble à l'image originale, plus cette preuve a de valeur.

D'autres avenues pourraient être explorées, en ce qui concerne le traitement des images de signatures manuscrites. En effet, des processus de traitement «hors-ligne» des signatures manuscrites permettent d'obtenir des descriptions de haut niveau de ces signatures, descriptions qui sont équivalentes à une compression indirecte. Par exemple, Ammar, Yoshida et Fukumura [Ammar et al., 1990] ont introduit une méthode de description hiérarchique des signatures manuscrites. Cette description prend en compte les caractéristiques d'une signature ainsi que les relations entre ses différentes parties composantes, organisées dans une structure hiérarchique.

Cette approche hiérarchique place la signature manuscrite au plus haut niveau de la représentation et chaque niveau inférieur contient de plus en plus de détails sur le niveau immédiatement supérieur. La signature est décrite en utilisant une description globale, représentée par une chaîne de caractères, tandis que la description locale est représentée par une structure arborescente. Les signatures ne peuvent pas être reconstituées à partir de leur description; toutefois, la description fournit une quantité suffisante d'information pour permettre de caractériser la signature et ses composantes.

Avec une telle méthode de description, un numéro biométrique personnel pourrait être crée, l'information descriptive pouvant être divisée entre ses deux sous-composantes, tel que décrit dans la sous-section 4.4.4.3. Comme cette méthode a été conçue premièrement pour servir à la vérification des signatures manuscrites, sans tenir compte de la quantité de données incluse dans chaque niveau de description, le nombre de niveaux dans la hiérarchie devra être gardé suffisamment bas, sans quoi, aucun effet de compression ne pourra être réalisé.

Dans le même esprit, Lee et Pan [Lee et Pan, 1992] proposent une méthode de représentation des signatures manuscrites basée sur les caractéristiques géométriques et topologiques décrivant les propriétés locales d'une signature. Ces caractéristiques sont extraites en employant, entre autres, des approximations polygonales et en

effectuant la segmentation des traits. Les caractéristiques géométriques et topologiques ont une haute tolérance aux variations de style et aux distorsions, ainsi qu'à un niveau limité de variations de translation et de rotation.

En utilisant des caractéristiques distinctes pour chacune sous-composante du numéro biométrique personnel, un ID-biométrique pourrait être construit. De cette façon, aucune partie de l'image de la signature manuscrite ne sera incluse dans cet identificateur biométrique, seules des informations descriptives étant incorporées.

4.4.5.3 Autres moyens biométriques

En poursuivant ce bref survol des solutions alternatives, d'autres méthodes d'identification biométrique peuvent être utilisées; une telle option serait de remplacer la signature manuscrite par des empreintes digitales; l'image de l'empreinte remplacerait alors l'image de la signature manuscrite contenue dans les signatures biométriques. Ou bien, en repérant sur une empreinte un certain nombre de points (habituellement une douzaine), nommés des minutiæ, une représentation fiable de la dite empreinte pourrait être reproduite. L'information à stocker devient alors minime.

L'utilisation des technologies biométriques continue de s'accroître au fil des ans, profitant d'une performance accrue accompagnée d'une diminution rapide des coûts. De plus en plus, la précision de l'identification et de l'authentification des usagers est reconnue et mise en valeur par des institutions bancaires, d'état et autres, comme élément clé de la réduction substantielle de la fraude et de l'accroissement de la confiance dans la sécurité informatique.

Après plusieurs années d'utilisation très limitée, les ventes d'applications biométriques commencent à prendre un essor sans précédent et, par conséquent, de plus en plus de fabricants importants de matériaux informatiques ont commencé à incorporer

de tels outils dans leurs claviers, guichets automatiques, ordinateurs personnels ou blocs-notes électronique. Des applications concrètes, tels que des systèmes d'enregistrement des électeurs, des permis de conduire, de contrôle de l'immigration ou de l'identité et de l'accès électronique, ont déjà été implantées dans plusieurs pays, incluant le Canada.

4.4.5.4 Autres aspects personnalisables

Un autre aspect configurable du système TRANZIX concerne les exigences de vérification. Ainsi, chaque entité transactionnelle peut décider et configurer sur mesure les limites des montants transigés au-dessus desquels une vérification automatique en-ligne doit être effectuée. Comme ceci implique évidemment un accroissement de la quantité de données transmise, échangée et à traiter, augmentant ainsi les coûts marginaux d'opération; il faut que le niveau de sécurité soit proportionnel à la valeur de chaque transaction.

Évidemment, le niveau de sécurité requis est corrélé directement avec la puissance de calcul et la largeur de bande disponible, ainsi qu'avec les coûts d'installation et d'opération, influençant ainsi le chiffre d'affaires total. Une considération spéciale doit donc être accordée à cet aspect pour obtenir la meilleure configuration possible pour chaque solution transactionnelle. De cette façon, la nature hautement configurable et personnalisable du système TRANZIX permet d'interchanger arbitrairement les modules de sécurité, tout en restant conforme aux spécifications de base du protocole de communication, afin d'obtenir la meilleure solution transactionnelle pour chaque application en particulier.

4.5 Conclusion

Voilà comment nous pouvons assurer la sécurité du système TRANZIX. Nous avons vu comment les communications et les protocoles transactionnels sont protégés par des moyens cryptographiques forts et comment la protection des instruments de transfert généralisé de valeurs est accomplie par un mécanisme qui contient autant des moyens cryptographiques que des moyens biométriques. De plus, une grande flexibilité est offerte quant aux mécanismes de personnalisation. Une méthode de personnalisation employant les images filtrées par pixelisation des signatures manuscrites des clients a été présentée en détail – puisque c'est cette méthode qui est utilisée par défaut dans notre design. Une autre méthode, utilisant une approche multi-résolution, a été aussi présentée comme alternative théorique et d'autres options ont aussi été brièvement discutées.

Ce chapitre nous a permis de présenter en détail la structure du système électronique de transport, transfert et d'échange numérique de valeurs; nous avons présenté son concept de base, ses acteurs, ainsi que les spécifications fonctionnelles pour chacune des entités, incluant le DFD, à plusieurs niveaux de raffinement. Par la suite nous avons proposé le design préliminaire du système, en introduisant son DH, et en décrivant ses interfaces avec l'environnement extérieur et la structure des données employées. Nous avons aussi discuté du traitement des exceptions, qu'elles soient dues aux erreurs ou pannes de fonctionnement ou à des fraudes. Enfin, nous avons décrit les mécanismes de protection de TRANZIX, en présentant les moyens cryptographiques de sécurisation ainsi que les moyens biométriques de personnalisation visant à renforcer la confiance des utilisateurs dans notre système.

CHAPITRE 5

DISCUSSION ET ANALYSE

Après avoir présenté en détail, dans le chapitre précédent, le nouveau système transactionnel TRANZIX, nous allons maintenant effectuer une première analyse du système, en étudiant plusieurs de ses éléments internes. Pour ce faire, nous avons réalisé un prototype squelettique d'une entité transactionnelle de TRANZIX qui nous permet d'évaluer les grandes lignes des performances du système.

Tout d'abord, nous décrivons ce prototype en analysant sa structure interne et ses composantes; nous allons présenter en détail les différentes étapes du protocole de transport des enveloppes virtuelles et du protocole transactionnel. Par la suite, nous introduisons quelques applications qui ont été implantées afin de tester et valider le prototype. D'autres applications sont proposées, permettant ainsi de montrer la grande flexibilité de TRANZIX et le grand éventail de problèmes que ce système pourrait résoudre. Nous illustrons ainsi l'utilité du nouveau système et faisons ressortir les avantages incontestables d'un outil transactionnel multi-fonctionnel. Enfin, nous discutons plusieurs caractéristiques du système et nous analysons certains résultats expérimentaux, notamment les temps de génération des clés cryptographiques et les temps de transaction.

5.1 Démonstration de la faisabilité

5.1.1 Design détaillé et réalisation d'un prototype

Pour démontrer la faisabilité de notre système électronique de transfert numérique de valeurs, nous avons construit un prototype expérimental. Nous l'avons intégré au réseau Internet par l'intermédiaire du Web et d'une interface avec un serveur et un fureteur, offrant ainsi la possibilité de transiger facilement des valeurs dans le monde virtuel. Pour ce faire, nous avons implanté le prototype expérimental sous la forme d'un ***module de facturation sécuritaire***, réalisé en langage Java. Comme ce module regroupe les éléments de base de la partie client – comprenant donc tant l'entité transactionnelle client que l'entité transactionnelle vendeur –, nous allons l'utiliser comme prototype nous permettant de simuler le comportement global du système et d'évaluer ainsi ses performances.

Deux protocoles se superposent afin d'acheminer correctement les transactions. Tout d'abord, un protocole de communication permet le transport des enveloppes virtuelles d'une entité transactionnelle à une autre; par-dessus cette couche, un protocole transactionnel de facturation spécifie la façon par laquelle des valeurs peuvent être véhiculées à l'aide de ces enveloppes virtuelles. Les valeurs de base transportées par ce prototype sont constituées de billets virtuels et de certificats numériques. En effectuant quelques légères modifications, d'autres valeurs pourraient aussi être transigées, telles que des jetons numériques, des pièces d'identité ou d'autres documents électroniques. Nous appelons ***objets virtuels*** toutes ces valeurs, qu'elles soient des produits ou des services.

Après avoir acheté (ou reçu) des billets numériques, l'acheteur peut activer son portefeuille virtuel en suivant un lien hypertexte payant dans un magasin virtuel. Il

achète alors des biens ou services à l'aide de son fureteur et de son logiciel transactionnel. Le portefeuille virtuel du vendeur contacte alors celui de l'acheteur en lui envoyant une requête de paiement pour la marchandise demandée. L'acheteur peut définir dans les préférences du logiciel, des limites prédéterminées en dessous desquelles il n'a plus besoin de confirmer chaque paiement qu'il doit effectuer (0.0015 $, par exemple). Une fois que la requête de paiement est approuvée par l'acheteur, un ou plusieurs billets numériques sont envoyés au vendeur, qui peut, optionnellement, les déposer immédiatement à la banque afin de vérifier sur-le-champ leur validité, prévenant ainsi toute tentative de dépenses multiples par copiage.

Le transfert de fonds s'effectue immédiatement, l'argent numérique étant transféré du disque dur de l'ordinateur de l'acheteur au disque dur du serveur du vendeur. Le vendeur peut choisir d'effectuer des transactions hors-ligne, afin d'augmenter la vitesse des transactions – pour les microtransactions, par exemple – et déposer les billets à la fin de la journée ou de la semaine. Le vendeur peut aussi définir dans les préférences de son logiciel, des limites prédéterminées en dessous desquelles il n'a plus besoin de vérifier chaque transaction auprès de la banque.

En mode en-ligne, le vendeur livre la marchandise à l'acheteur après avoir vérifié le paiement auprès de la banque. En mode hors-ligne, la marchandise peut être livrée avant la vérification. Ainsi, selon l'importance de la transaction, le vendeur aura le choix de l'effectuer en-ligne ou hors-ligne.

5.1.2 Le module de facturation sécuritaire

Un prototype du système TRANZIX a été implanté en langage Java et utilisé pour facturer des micropaiements. Ayant plus de 5000 lignes de code distribuées dans plus de 50 classes, le prototype a permis de mesurer plusieurs paramètres

transactionnels, tels que le temps de génération des clés cryptographiques, le temps de transaction ainsi que l'influence de la longueur des clés d'encryptage sur ces valeurs. Conformément aux spécifications TRANZIX, la granularité de la devise utilisée peut être arbitrairement petite. Pour démontrer ce fait, nous avons implanté dans le cadre du module de facturation sécuritaire un montant «atomique» (indivisible) minimal de 0.01 cents (une centième de cent), soit 0.0001 $. La monnaie représentée dans notre système est le dollar canadien, émis avec une couverture complète («*swap* 1 à 1»), c'est-à-dire, que pour chaque dollar réel qui entre dans le système électronique de paiement, un seul dollar virtuel est émis et peut circuler jusqu'à ce que le dollar réel soit retiré du système. À ce stade-ci, il serait inopportun, à notre avis, de créer une masse monétaire additionnelle non-couverte, vu l'état de développement du système électronique de transfert numérique de valeurs et le vide juridique qui couvre ces nouveaux aspects de l'économie et des systèmes bancaires.

Pour pouvoir effectuer des calculs préliminaires sur les performances du système, regardons de plus près la structure du module de facturation sécuritaire du système TRANZIX. Sans entrer dans les détails de design, nous allons survoler rapidement ses sous-modules internes et externes ainsi que le PTEV et le protocole transactionnel. En suivant de près le modèle des centres de traitement présent dans le DH, nous avons construit plusieurs ensembles de sous-modules[1] internes; afin de pouvoir distinguer entre les différentes composantes du logiciel, nous avons décidé de les regrouper en deux ensembles: toutes les classes Java intrinsèquement reliées au fonctionnement d'un module sont regroupées en ce que nous appelons les ***sous-modules internes***; ces sous-modules ont chacun une ou plusieurs tâches à effectuer, ce qui permet de fragmenter et ainsi de mieux gérer le travail de chaque composante. Par ailleurs, toutes les classes et les scripts qui servent d'interfaces entre notre prototype et

[1] Notons, cependant, qu'ici, le terme sous-module représente une ou plusieurs classes en langage Java et ne suit pas nécessairement de façon directe la description générale du système complet présentée dans le DH.

un serveur Web ou entre notre prototype et ses applications sont regroupées dans ce que nous appelons les ***sous-modules externes***. Tel que prévu par les spécifications TRANZIX, le client et le vendeur utilisent le même logiciel de facturation sécuritaire pour transiger. Nous présentons dans les pages qui suivent, d'une part, les deux ensembles de sous-modules, et d'une autre part, les protocoles qui régissent les échanges.

5.1.2.1 Les sous-modules externes

Cet ensemble de sous-modules regroupe seulement trois éléments: le pseudo-module banque, l'interface Web et le contrôleur d'application. Tout d'abord, le pseudo-module Banque contient une seule classe (`Banque.class`) qui est à toutes fins pratiques une coquille donnant constamment des réponses positives. Ce sous-module comprend un serveur à fils d'exécution multiples (*multi-thread*), qui écoute sur un port de communication, attendant une ou plusieurs connexions, qu'elles soient concomitantes ou non. Une fois la communication établie, le serveur accepte et valide toutes les requêtes reçues. L'implantation complète des fonctions requises par cette entité, incluant la gestion complète des adhésions, la gestion des comptes, ainsi qu'une base de données solidement protégée par encryptage, dépasse le cadre de notre mandat.

Un deuxième élément de cet ensemble est constitué par l'interface du module de facturation sécuritaire du système TRANZIX avec le Web. L'interface est constituée d'un script (`interface.cgi`) – écrit en langage ShellScript – relativement court mais complexe. Concrètement, il s'agit de l'intermédiaire entre le module de facturation et un autre programme, plus précisément, le serveur Web d'un magasin virtuel. L'interface permet ainsi au serveur Web de démarrer localement un module de facturation, en utilisant un portefeuille virtuel local – qui doit avoir, pour des raisons de sécurité, le même UID (identificateur d'usager) que l'UID du logiciel. Le module de facturation est ainsi démarré automatiquement en arrière-plan et il cesse toute activité

une fois la transaction accomplie. La complexité de ce sous-module réside d'une part au niveau de protection et d'accessibilité qu'il doit fournir, et d'autre part, au niveau des réponses qu'il doit produire pour chaque connexion avec un client. Tout d'abord, le module doit être accessible à partir d'un fureteur, donc lisible par tout le monde; par contre, les objets virtuels («la marchandise») offerts doivent être protégés contre tout accès non-autorisé, seul l'utilisateur qui a payé pourra y avoir accès, et seulement une fois. Le sous-module doit aussi vérifier le montant de la transaction avant d'effectuer l'appel au module de facturation, en lisant un fichier protégé contenant les montants exacts établis par le vendeur. Finalement, il doit afficher une réponse en format HTML, lisible par un fureteur, réponse accompagnée par des explications, nécessaires surtout pour les transactions qui n'ont pas réussi.

Enfin, le troisième élément externe est représenté par le contrôleur d'application: cet élément peut être constitué par une collection de scripts et de programmes Java – ou autres. Dans notre cas, il s'agit de deux scripts, un qui contrôle effectivement l'application et un autre, intermédiaire, qui sert à fournir un prix en mode interactif, en fonction des réponses données par le client. Non seulement le prix doit être affiché au client, mais il doit aussi être écrit dans la liste protégée des prix, mentionnée plus haut. En ce qui concerne l'application proprement dite, des instructions spécifiques peuvent être incluses dans le script pour la lancer et la contrôler, sans aucun paramètre spécial.

5.1.2.2 Les sous-modules internes

Pour pouvoir effectuer des transactions, tout portefeuille virtuel doit être initialisé. C'est justement le but du premier sous-module interne, le sous-module d'initialisation; notons que le portefeuille virtuel est physiquement constitué d'un répertoire, appelé `comptes/`, contenant plusieurs fichiers et sous-répertoires. Deux tâches très importantes sont sous le contrôle direct de ce sous-module: le déploiement du

logiciel et la génération des clés cryptographiques. Dans un premier temps, pendant le déploiement, lors du tout premier contact du client avec le logiciel, ce dernier «étudie» l'environnement dans lequel il se trouve et essaie de créer automatiquement tous les répertoires, les sous-répertoires et les fichiers d'autoconfiguration et de travail nécessaires pour démarrer et travailler correctement. Une configuration générale, de base, est fournie avec le logiciel afin d'éviter au client les risques d'une première configuration erronée. Une vérification de l'intégrité de la structure des fichiers est effectuée lors du déploiement, ce qui permet d'arrêter le fonctionnement des distributions logicielles corrompues: si un fichier est manquant (par exemple le fichier `comptes/info-ban.txt`) l'exécution est interrompue automatiquement et l'usager est informé et avisé de contacter la banque. Si la vérification de l'intégrité est réussie, le déploiement peut continuer et sera suivi par la génération d'une paire de clés cryptographiques. Par la suite, à chaque fois que l'usager démarre le logiciel, une vérification de l'intégrité de la structure du portefeuille virtuel est effectuée, afin de permettre la détection de toute erreur ou de toute utilisation volontairement incorrecte ou frauduleuse avant de commencer à négocier une transaction.

Le sous-module de gestion du portefeuille virtuel est le cœur du module de facturation. Ce sous-module est vital pour le fonctionnement du logiciel, il s'occupe de toutes les opérations transactionnelles et c'est le seul à accéder aux billets virtuels dans le portefeuille local. Les tâches qui sont réalisées par ce sous-module sont: l'initialisation du portefeuille virtuel à chaque démarrage du logiciel; la manipulation des billets numériques; les paiements; la facturation et la réception des transferts; la récupération des données résultant d'une transaction incomplète.

Physiquement, chacune de ces tâches est réalisée par une ou plusieurs méthodes[2] à l'intérieur d'une seule classe, `GestionPortefeuille.class`. Tout d'abord, lors de chaque démarrage du logiciel, une initialisation du portefeuille virtuel est effectuée,

[2] Fonctions ou sous-fonctions dans un langage orienté objet.

afin de s'assurer de l'intégrité des données et d'éviter l'utilisation des données/billets corrompus avant toute transaction. Pour ce faire, un fichier index (dans le répertoire `comptes/cash/`) est lu et comparé avec l'ensemble des billets existants, lors de chaque transaction. L'index contient le nombre de billets se trouvant dans le portefeuille virtuel, leur valeur, ainsi que le montant total, résultant de l'addition de chaque montant individuel. Cet index est en quelque sorte la trace des opérations mathématiques effectuées sur le portefeuille. Le traitement des billets a lieu en plusieurs étapes: premièrement le sous-module lit le montant de chaque billet, ces billets ne se trouvent pas nécessairement arrangés dans un ordre établi dans le portefeuille.

Une fois qu'un ou plusieurs billets ont été sélectionnés, dans le cas d'un paiement, ou que des enveloppes virtuelles ont été décomposées en billets, dans le cas d'une facturation d'un transfert de fonds reçu, cette partie du sous-module se charge de leur déplacement entre les différents sous-répertoires du portefeuille virtuel. Ce déplacement utilise la méthode `renameTo()` du langage Java: il crée donc un nouveau fichier à l'endroit demandé et efface le fichier à déplacer. Pour nommer ou renommer un fichier, nous utilisons une méthode précise, standardisée. La convention de noms de fichiers contenant des billets adoptée dans le portefeuille est la suivante: chaque billet, dès qu'il est reçu, peu importe le moyen de transport – disquette, courrier électronique ou transaction en-ligne – est transféré dans le répertoire `comptes/cash/` (après plusieurs étapes décrites plus bas). Il reçoit comme nom un nombre entier, égal au nombre de billets déjà dans le répertoire, plus un, en commençant par 1. L'extension de ce nom sera la chaîne alphanumérique `.bil`, `.dep` ou `.fin` (en fonction du statut du billet, billet valide, billet déposé ou billet faisant partie d'une transaction non-finalisée). Par exemple, si le portefeuille contient déjà deux billets (`1.bil` et `2.bil`), lorsqu'un troisième est reçu, son nom sera `3.bil`.

Regardons de plus près la structure interne du portefeuille virtuel. Il s'agit tout simplement d'une structure arborescente qui a sa racine dans le répertoire principal

de la structure du module de facturation sécuritaire. Cette racine est appelée `comptes/`, comme nous l'avons déjà brièvement mentionné, et contient quatre sous-répertoires et un fichier. Voyons la structure complète du portefeuille, avec tous ses sous-répertoires et ses fichiers (chaque signe «+» représente un niveau inférieur dans l'arborescence):

```
comptes/ (la racine du portefeuille)
+----| info-ban.txt (informations de configuration - format texte, ASCII)
+----| cash/ (répertoire des billets numériques)
+----+----| index (fichier d'index des billets, en format binaire)
+----+----| 1.bil (un billet)
+----+----| 2.bil (un deuxième billet)
+----+---- dep/ (répertoire des billets dépensés - vidé une fois la banque contactée)
+----+----+----| 1.dep (un billet déjà dépensé)
+----+---- fin/ (répertoire des transactions non finalisées)
+----+----+----| 1.fin (un billet faisant partie d'une transaction non finalisée)
+----+---- pay/ (répertoire tampon pour les paiements)
+----+---- rec/ (répertoire tampon pour les facturations et les autres transferts reçus)
+---- cles/ (répertoire des clés cryptographiques)
+----+----| banque.txt (clé publique de la banque - format texte, ASCII)
+----+----| banque.bin (clé publique de la banque - format encrypté, binaire)
+----+----| cles-asc.txt (clé publique de l'usager - format texte, ASCII)
+----+----| cles-pub.bin (clé publique de l'usager - format encrypté, binaire)
+----+----| cles-sec.bin (clé secrète de l'usager - format encrypté, binaire)
+----+----| usager (les données d'identification de l'usager - nom, adresse, ...)
+---- logs/ (répertoire des fichiers de trace)
+----+----| AC-PAYM (limite des paiements automatiques)
+----+----| AC-TRAN (limite des transferts à recevoir)
+----+----| CL-VERI (limite des vérifications à effectuer en-ligne)
+----+----| log (fichier de trace principal)
+---- transactions/ (répertoire des transactions)
+----+----| pay (fichier de trace des paiements)
+----+----| rec (fichier de trace des transferts reçus)
+----+----| recus (fichier de trace des reçus de paiement)
+----+----| transactions (fichier de trace de toutes les transactions)
```

Le fichier contenu dans le répertoire principal du portefeuille virtuel, appelé `comptes/info-ban.txt` contient des informations de configuration concernant l'émetteur de la devise utilisée, donc la banque qui a fourni le logiciel. Ces informations incluent, tel que spécifié dans le Chapitre 4, les coordonnées de l'émetteur, ainsi que la clé publique

de la banque. En ce qui concerne les billets numériques, tel que prévu dans les spécifications de TRANZIX, en plus des informations de base encryptées par la banque, nous avons ajouté des «informations lisibles», non-encryptées, qui permettent aux usagers d'avoir des informations sur chaque billet, tels que son numéro de série, sa valeur nominale, sa granularité, sa date d'expiration, etc. Seul un minimum d'information a été retenu afin de minimiser la quantité d'information résidant dans le billet, car il faut garder à l'esprit le fait que la taille des billets s'accroît avec chaque transaction, de nouvelles signatures étant rajoutées automatiquement.

Continuons la description des tâches réalisées par ce sous-module. Si la transaction courante à traiter est un paiement, le sous-module trouve, à l'aide d'un ***algorithme de paiement***, une combinaison de billets – parmi plusieurs combinaisons possibles – qui correspond au montant exact de la transaction. Dans la version actuelle du prototype, si aucune combinaison n'est trouvée, c'est-à-dire si le client n'a pas les bonnes coupures pour effectuer le paiement, afin d'éviter de «faire la monnaie», la transaction échoue et un message sera transmis aux deux entités transactionnelles en cause. La limitation causée par ce choix de design, de ne pas offrir la possibilité de retourner la monnaie virtuelle, est largement compensée par les gains obtenus à la fois au niveau de la vitesse (moins d'étapes dans le protocole de facturation, moins de calculs cryptographiques à faire, moins d'enveloppes virtuelles et de messages transactionnels à transmettre, moins de temps de communication et de largeur de bande requise) et au niveau de la complexité du protocole de facturation.

L'algorithme de paiement emploie trois méthodes et retourne la première combinaison de billets trouvée, aucune optimisation n'étant effectuée à ce moment. Une fois les billets trouvés, chaque billet est signé, et une enveloppe virtuelle est composée en regroupant les billets signés; après l'étape de construction, cette enveloppe passe à l'étape d'encryptage, pourvu que la clé publique du destinataire soit disponible. Finalement, le résultat est mis temporairement dans le sous-répertoire `comptes/cash/pay/`

afin qu'un autre sous-module puisse y avoir accès pour le transmettre au destinataire. La méthode principale qui s'occupe de toute cette suite de traitements est la méthode `payer()` de la classe `GestionPortefeuille.class`. Si, par contre, la transaction courante à traiter est une facturation et la réception d'un transfert de fonds, le sous-module prend les billets résultant du décryptage (si l'enveloppe virtuelle a été encryptée) et de la décomposition de l'enveloppe reçue, à partir du sous-répertoire `comptes/cash/rec/` et les transfèrent à leur place, dans le répertoire `comptes/cash/` en s'assurant de leur donner des noms corrects, tels que prévu par la convention établie.

Nous nous sommes rendus compte du fait que parfois, pour des raisons différentes, la communication est interrompue avant qu'une transaction ne soit finie. Malheureusement, même s'il reste des traces de la transaction, les billets sont perdus ou difficilement retrouvables. À quel niveau dans l'exécution du protocole l'interruption de la communication est-elle arrivée ? À qui appartient désormais les billets contenus dans les enveloppes virtuelles ?

Pour cette raison, ainsi que pour les raisons décrites dans le chapitre précédent, nous avons implanté des méthodes de sauvegarde et de recouvrement, en sachant que nous ne pouvons pas nous permettre de perdre même une fraction de cent à cause des erreurs de transmission, de fonctionnement ou autres. L'argent numérique se trouve dans le répertoire `comptes/cash/`; ce répertoire contient aussi l'index des billets, ainsi que quatre autres sous-répertoires: deux sous-répertoires tampon, et deux sous-répertoires de sécurité: des copies de chaque billet dépensé sont effectuées lors de chaque paiement et ces copies sont déposées dans le sous-répertoire `comptes/cash/dep/`. Ceci permet de s'assurer qu'aucun billet ne sera pas perdu lorsqu'une transaction ne pourra pas être terminée pour une raison ou pour une autre. Lors de la prochaine connexion auprès de la banque, ces données pourraient être synchronisées avec les données du compte en banque et le sous-répertoire pourrait être vidé de façon transparente.

En ce qui concerne les transactions qui n'ont pas été finalisées, la solution que nous proposons est de construire une méthode (la méthode `finaliser()` dans `GestionPortefeuille.class`) qui surveille l'état du portefeuille virtuel et détecte toute anomalie causée par une transaction incomplète. De cette manière, si lors du démarrage ou de la fin d'une séance d'utilisation du logiciel, une ou plusieurs transactions sont détectées comme étant non-complétées (à l'aide des fichiers temporaires non-effacés qui sont détectés à cet effet), ces messages seront décomposés et les billets qui sont retrouvés sont mis dans le sous-répertoire `comptes/cash/fin/`. De cette manière, nous nous donnons la possibilité de pouvoir finaliser la transaction ultérieurement, en-ligne, à l'aide de la banque, qui pourrait trancher de façon définitive le problème d'appartenance d'un billet donné – en fonction de l'étape à laquelle la transaction interrompue s'est rendue. Ce sous-répertoire sera à son tour vidé dès que les données seront synchronisées avec la banque. En employant ces deux méthodes, nous pouvons nous assurer qu'aucun billet, peu importe sa valeur, ne sera perdu et ce, peu importe l'erreur qui apparaît.

Le sous-module de gestion de la sécurité est un élément constitué d'une collection de classes Java, structurée autour de la librairie Cryptix. Le sous-module prend soin de tous les calculs et toutes les opérations cryptographiques que ce soit des opérations uniques, comme la génération des clés, ou récurrentes, comme l'encryptage ou le décryptage. Ainsi, la sécurité des communications est assurée en encryptant les messages transmis. Notons que, afin d'assurer à l'usager la possibilité d'effectuer des transactions de façon automatique – par exemple en laissant le logiciel s'occuper de transactions reçues par le serveur Web sans assistance de la part de l'usager – son mot de passe est requis sur le disque dur. Afin de ne pas l'écrire en clair, une méthode de la classe `cles.class` prend le mot de passe de l'usager saisi lors de la génération des clés et l'écrit dans un fichier temporaire qui est compilé dans une classe Java sur mesure, prête à le fournir aux méthodes autorisées à l'utiliser; cette classe est évidemment différente d'un usager à un autre. D'autres moyens pour stocker le mot de passe de l'usager, encore plus sécuritaires, pourraient être inclus dans une éventuelle version commerciale.

La gestion de la communication est réalisée à l'aide d'un sous-module comportant trois fonctions: la composition/décomposition des enveloppes virtuelles, la transmission ou l'écoute en tant que serveur et la transmission ou la réception en tant que client. Il est utile à ce niveau de clarifier l'aspect «communications» dans le nouveau système proposé. Les termes client/serveur sont utilisés ici pour désigner des entités de l'architecture réseau portant le même nom. Tous les intervenants possèdent un logiciel TRANZIX; du point de vue de la communication, chaque entité transactionnelle possède à l'intérieur de son logiciel un serveur qui lui permet d'écouter sur le réseau pour capter une éventuelle requête de connexion de la part d'un autre logiciel TRANZIX, tel qu'un module de facturation sécuritaire. Sans un tel serveur, les usagers pourraient seulement contacter la banque, sans pouvoir se contacter entre eux. Par contre, l'entité banque nécessite un serveur spécial. En plus du serveur [de communication] qui reçoit et gère les communications, elle doit posséder un serveur capable de traiter de façon très prompte les diverses requêtes de différents types effectuées par les clients et de gérer les différentes bases de données contenant les comptes, les clés, les ID-biométriques etc.

Prenons tout d'abord la composition/décomposition des enveloppes virtuelles. Pour effectuer un paiement, plusieurs billets doivent être regroupés dans un fichier temporaire – l'enveloppe virtuelle; en rajoutant l'en-tête contenant le montant de la transaction, la description et le nombre de billets inclus, nous obtenons un message qui sera envoyé encrypté ou non au destinataire de la transaction, que ce soit directement, par connexion TCP/IP, ou indirectement, par courrier électronique ou par disquette.

Une fois rendue au destinataire, l'enveloppe virtuelle sera décomposée en lui enlevant l'en-tête, son intégrité sera vérifiée et les billets seront séparés. Les méthodes qui s'occupent de ces tâches se trouvent dans la classe `GestionEnveloppes.class`. De façon concrète, nous avons déjà mentionné le fait que, du

point de vue du réseau, le logiciel remplit en même temps le rôle d'un serveur et le rôle d'un client. En ce qui concerne son premier rôle, un serveur à fils d'exécution multiples (*multi-thread*) est défini, ce qui permet d'écouter sur un port de communication et de démarrer en parallèle plusieurs fils (*threads*) d'exécution si une autre demande se présente avant que la première ne soit traitée et finalisée.

Notons un artifice au niveau de l'implantation du serveur de communication: comme la méthode Java qui écoute et accepte des connexions réseau, la méthode `accept()`, suspend le flot d'exécution et attend indéfiniment une connexion, bloquant ainsi toute autre activité, nous avons dû utiliser un temps d'arrêt (*timeout*) afin d'interrompre le serveur pour pouvoir le repartir périodiquement, à des intervalles très courts. Ceci permet de contourner le blocage et de donner la possibilité à d'autres fonctions de s'exécuter, étant donné que l'écoute doit se faire en arrière-plan. Une fois qu'une connexion est reçue et que la communication est établie, le contrôle suivra le protocole de transport des enveloppes virtuelles (décrit dans la sous-section 5.1.2.4) et celui de la facturation (décrit dans la sous-section 5.1.2.5) et complétera le traitement de cette connexion; la connexion sera alors fermée, le résultat sera écrit dans le fichier principal de trace et présenté au client. La protection des données et des structures employées est réalisée en utilisant, entre autres, des fichiers de blocage (*lock files*) qui arrêtent l'exécution de toute modification ou activité sur une variable en particulier ou sur une structure de données en général. De cette façon nous nous assurons qu'un seul fil d'exécution peut accéder à ses propres données et qu'un seul fil d'exécution peut modifier des variables globales à un moment donné. De plus, nous utilisons des procédures de synchronisation des fils d'exécution à l'aide de sémaphores. Nous délimitons ainsi clairement le rayon d'action de ces fils et un gestionnaire central d'exécution peut même suspendre un ou plusieurs fils lorsque des modifications importantes dans la structure de données ont lieu, tels que l'écriture du nouveau solde. Vu le temps nécessaire pour une telle écriture dans la mémoire du système, le coût engendré par une telle interruption de l'exécution est négligeable.

Du côté client, une connexion avec le serveur de l'autre entité transactionnelle est tentée à deux reprises, à un intervalle de temps très court. La deuxième tentative est utile si jamais la première arrive juste au moment où le serveur du destinataire se recharge. Si la connexion échoue pour les deux essais, un message indiquant que le destinataire n'est pas présentement en-ligne est affiché. Si la connexion peut être établie, les messages échangés suivent de façon très stricte le scénario imposé par le protocole TRANZIX. Tout message reçu qui ne fait pas partie de l'ensemble des messages TRANZIX (message hors-contexte) ou qui ne correspond pas à l'étape transactionnelle à laquelle le logiciel s'est rendu (message hors-séquence), déclenche l'envoi d'un message de fin de dialogue et la clôture du canal de communication.

La gestion des fichiers de trace est réalisée par un autre sous-module, qui offre ainsi un moyen efficace de retracer les actions entreprises par l'usager, en les enregistrant dans des fichiers de trace; ces fichiers pourront servir de référence, d'exemple ou de preuve. Plusieurs types d'information sont enregistrés; tout d'abord toutes les informations concernant les transactions du client seront enregistrées: le fichier `comptes/transactions/transactions` enregistre toutes les transactions effectuées. Voici un très court extrait:

```
#5 Mar 18 Aou 1998 a 17:11:09 P $1.0 Tester une transaction
#6 Mar 18 Aou 1998 a 17:11:24 R $1.0 Tester une transaction
```

Il est facile de remarquer un numéro de transaction courante, la date et l'heure, le type («P» pour paiement, «R» pour transfert reçu, «I» pour initialisation) et le montant de la transaction ainsi que sa description. Dans cet exemple simplifié, le logiciel a enregistré un paiement de 1 dollar pour «Tester une transaction», mardi le 18 août 1998, à 17 heures, 11 minutes; quelques secondes plus tard, un paiement d'un dollar a été reçu – la transaction était avec soi-même, comme le démontrent le montant et la description. Le fichier `comptes/transactions/pay` enregistre seulement les paiements; ainsi, toutes les informations contenues dans les champs d'une ligne seront les mêmes

que celles du fichier précédent, à l'exception du type, qui sera toujours «P». Le fichier `comptes/transactions/rec` enregistre seulement les facturations et les transferts reçus – de la même manière, le type sera toujours «R». Le fichier `comptes/transactions/recus` enregistre seulement les reçus de paiement qui ont été signés numériquement et envoyés par le destinataire d'un paiement; ces reçus sont standardisés et contiennent la date, l'heure, le montant et la description de la transaction. Le message ainsi composé est signé et peut donc représenter soit une preuve de paiement pour l'acheteur, soit une preuve de réception des fonds pour le vendeur. Finalement, le fichier `comptes/logs/log`, fichier principal de trace, enregistre toutes les actions de l'usager, incluant le solde au démarrage, au début et à la fin d'une transaction. Voici un très court extrait de ce dernier fichier:

```
Mar 18 Aou 1998 a 16:11:36 - ----START----
Mar 18 Aou 1998 a 16:11:44 - Fin de l'initialisation.
Mar 18 Aou 1998 a 16:11:45 - Index billets lu.
Mar 18 Aou 1998 a 16:11:45 - Total initial = 4.0147
Mar 18 Aou 1998 a 16:12:24 - Attente...
Mar 18 Aou 1998 a 16:12:25 - Effectuer requete: =0.0001$Test Linux
...
```

Compte tenu du fait que ces fichiers de trace peuvent, avec le temps, devenir très volumineux, et par conséquent occuper beaucoup d'espace sur le disque, il est de la responsabilité de l'usager de les archiver ou de les effacer régulièrement. Une fonction d'archivage pourrait être incluse éventuellement dans une future version commerciale de TRANZIX.

Finalement, les fonctions locales servent essentiellement à configurer ou à reconfigurer le logiciel. Les options qui peuvent être configurées, modifiables à l'aide de ces fonctions locales, sont les suivantes: la limite maximale des paiements automatiques (c'est-à-dire le montant maximal en dessous duquel l'acheteur ne veut plus être consulté pour une autorisation), le choix pour l'acceptation automatique des facturations et des transferts à recevoir (si le client désire être consulté pour accepter un

éventuel montant qu'il pourrait recevoir), la limite maximale des paiements qui ne seront pas vérifiés en-ligne avec la banque, le mode de communication (par connexion directe TCP/IP, par courrier électronique, disquette, etc.), ainsi que le numéro de port de communication à utiliser. Une attention particulière doit être portée aux autorisations de paiement car des prélèvements automatiques pourront ainsi être effectués à partir du compte de l'usager. Une liste de commandes disponibles ainsi qu'un pointeur vers le manuel d'usager en-ligne est aussi fourni.

La description de toutes ces options a été effectuée en détail dans le manuel d'utilisation [Ureche et Plamondon, 1999a]. Pour rester à un niveau strictement technique, mentionnons que certaines de ces options sont «volatiles» (notamment le choix du mode de communication et du numéro de port), c'est-à-dire, leur choix sera maintenu seulement pendant le fonctionnement courant du logiciel. Les autres choix d'options sont «permanentes», c'est-à-dire, le choix effectué est sauvegardé sur le disque dur et le logiciel prendra note de ces options lors du prochain démarrage. En ce qui concerne cette sauvegarde, le logiciel utilise les fichiers suivants: `AC-PAYM`, qui contient un nombre réel représentant la limite maximale des paiements pré-autorisés (0 pour aucun paiement autorisé d'avance); `AC-TRAN`, qui contient un fanion indiquant l'acceptation automatique des facturations et des transferts de fonds à recevoir; `CL-VERI`, qui contient un nombre réel représentant la limite maximale des transferts reçus qui ne seront pas vérifiés automatiquement (en-ligne) auprès de la banque (cas particuliers: 0 indique que tout transfert reçu sera vérifié en-ligne avec la banque, 1000 indique qu'aucun transfert reçu ne sera vérifié en-ligne avec la banque). Ces fichiers sont écrits dans le répertoire `comptes/logs/`.

5.1.2.3 Comment s'effectue la facturation ?

Regardons d'abord ce qui se passe du côté de l'acheteur. Après avoir installé le module de facturation sécuritaire du système TRANZIX sur le disque local,

logiciel qui s'auto-déploie, en écrivant les fichiers nécessaires et en générant les clés afférentes, l'acheteur met le logiciel en marche. Il peut choisir de démarrer le module de facturation en mode texte ou en mode graphique. Ainsi, le mode texte offre l'avantage de permettre au logiciel d'être appelé automatiquement à partir d'un autre programme, tel qu'un script ou un serveur Web. Par ailleurs, l'avantage du mode graphique réside évidemment dans la facilité d'utilisation qu'il confère.

Une fois que l'acheteur décide d'acheter un objet virtuel, en suivant un lien payant dans le site Web du vendeur, il déclenche le module de facturation du magasin, qui lui envoie une requête de paiement; si l'acheteur accepte de payer, son logiciel essaye de construire le paiement avec les billets disponibles dans son portefeuille virtuel. Si les fonds nécessaires ne sont pas disponibles, la transaction échoue. Par contre, si les fonds sont disponibles, le logiciel les envoie au vendeur et il attend une confirmation. En supposant que la transaction a été réalisée correctement, cette confirmation arrivera sous la forme d'un reçu de paiement (qui s'ajoutera au fichier `comptes/transactions/recus`) démontrant que les fonds ont été reçus. En même temps, le client recevra soit directement l'objet virtuel (qu'il s'agisse d'un accès à un espace protégé, un mot de passe, etc.), soit un jeton numérique montrant que l'acheteur a le droit de recevoir l'objet [virtuel ou réel] en question.

Du côté du vendeur (et du serveur Web détenant les objets virtuels), le même logiciel s'installe de façon similaire et reste en attente. Une fois que le lien de paiement est accédé, le serveur Web renvoie, par l'intermédiaire de l'interface, la requête au logiciel, qui la décompose, et envoie une requête de paiement TRANZIX au client. Si les fonds nécessaires sont reçus, alors, en fonction des options de configuration interne ou des commandes manuelles reçues de la part du vendeur, le logiciel peut décider soit d'accepter les billets tels quels, soit de les déposer directement auprès d'une banque, et de les vérifier par la même opération. Sur réception de la confirmation de la réussite du transfert, le logiciel envoie le reçu directement au client,

et de plus, par l'intermédiaire de l'interface et du contrôleur d'application, il lui envoie l'objet virtuel: soit en lui envoyant une information (un mot de passe, etc.), soit en agissant comme point de transit entre le client et l'application désirée.

5.1.2.4 Le protocole de transport des enveloppes virtuelles

Un survol rapide du protocole de communication TRANZIX nous permet de montrer quelles sont les principales étapes de bas niveau nécessaires à l'acheminement correct et sécuritaire d'une transaction. Le PTEV, protocole de transport des enveloppes virtuelles introduit au chapitre précédent, se superpose au protocole TCP, à la couche immédiatement supérieure. C'est à toutes fins pratiques une machine à états qui détermine la suite des actions qui doivent être entreprises en réponse à des messages reçus. Voici un survol rapide de ces états:

Côté serveur (du logiciel de l'acheteur):

- Écoute pour une éventuelle connexion;
- Réception et acceptation d'une connexion;
- Réception d'une requête de transaction;
- SI la requête est acceptée: réception de la clé publique du destinataire;
  SINON: la transaction échoue
- Envoi au destinataire de la clé publique;
- Envoi de l'enveloppe virtuelle;
- Réception du reçu;
- Démarrage éventuel de l'application;
- Fin de la communication.

Côté client (du logiciel du vendeur):

- Requête de connexion;
- Requête de transaction;

- Envoi de la clé publique;
- Réception de la clé publique du destinataire;
- Réception de l'enveloppe virtuelle;
- Composition et envoi du reçu;
- Démarrage du contrôleur d'application;
- Fin de la communication.

Notons que ce protocole de communication se trouve à un niveau d'abstraction inférieur au protocole transactionnel, et concerne seulement la manière par laquelle les enveloppes virtuelles sont acheminées d'une entité transactionnelle à une autre. À l'aide de ce protocole, nous pouvons introduire au niveau immédiatement supérieur, un protocole transactionnel, présenté dans la sous-section suivante.

5.1.2.5 Le protocole transactionnel de facturation

Basé sur le protocole de communication que nous venons d'introduire, le protocole transactionnel de facturation permet d'effectuer une transaction en s'occupant du traitement des enveloppes virtuelles et de leur contenu. Par souci de clarté, nous allons énumérer les étapes du protocole transactionnel de facturation. Pour aider à sa compréhension, la Figure 5.1 montre graphiquement le protocole en son entier. Voici l'explication de la figure comprenant les neuf étapes du protocole:

0. L'acheteur arrive dans la page d'accueil du vendeur – le serveur Web du vendeur transmet la page d'accueil;
1. L'acheteur choisit le lien «payant»;
2. La requête de transaction est reçue par le serveur Web et renvoyée au vendeur par l'intermédiaire de l'interface;
3. Le vendeur envoie à l'acheteur une requête de paiement;

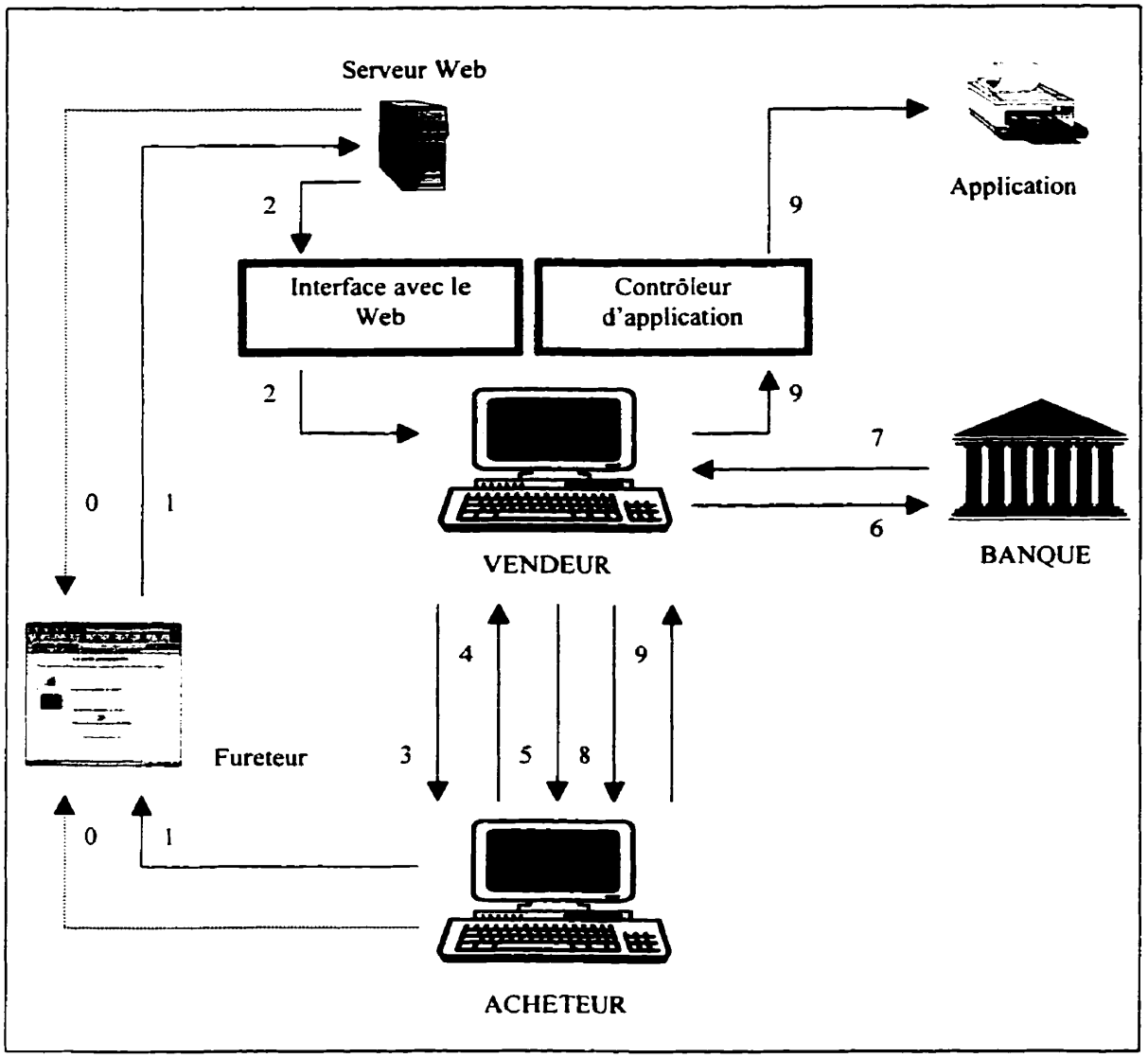

Figure 5.1 – *Le protocole transactionnel de facturation*

4. L'acheteur répond en transmettant:
   - soit l'enveloppe virtuelle contenant les billets => la transaction peut continuer;
   - soit un message d'annulation de la transaction => la transaction échoue;

5. Une confirmation de réception de l'enveloppe virtuelle est envoyée à l'acheteur;
6. [Optionnel] Le vendeur peut effectuer la vérification et le dépôt du paiement auprès d'une banque participante;
7. [Optionnel] La banque répond:
   - soit par une confirmation => la transaction peut continuer;
   - soit par un message d'erreur => la transaction échoue;
8. Le vendeur répond:
   - soit en envoyant le reçu de la transaction et l'objet virtuel acheté ou un jeton numérique => la transaction a réussi et prend fin;
   - soit en envoyant un message d'erreur => la transaction échoue;
9. Avec son jeton, le client peut accéder à l'objet virtuel, à l'aide d'un contrôleur d'application.

Sur des ordinateurs munis de microprocesseurs Pentium P100 à 100 MHz, tout ce processus peut prendre environ quelques dizaines de secondes ou moins, si les usagers connaissent déjà la procédure. La partie la plus longue est le transfert de fonds, qui prend autour de vingt secondes, mais cette mesure empirique dépend grandement de la longueur des clés utilisées.

5.2 Applications

Regardons en premier lieu quelques applications du système électronique de transfert numérique de valeurs, implantées à l'aide du module de facturation sécuritaire. Par la suite, nous allons présenter quelques applications théoriques dans lesquelles notre système aura, à notre avis, une utilité évidente.

Qu'est ce que le système peut facturer ? Tout ce qui circule sur un réseau numérique de communication. Des données, des informations, de l'accès à des pages d'un site Web, du temps d'utilisation de programmes exécutables (des calculs, forums de discussion, etc.), ainsi que l'accès à des ressources physiques – par l'intermédiaire d'un réseau intranet et ses périphériques –, tel que le contrôle de l'impression. En échange de ces objets virtuels, un paiement est envoyé de l'acheteur au vendeur en-ligne ou hors-ligne.

Afin de permettre d'illustrer le fonctionnement et l'utilité du module de facturation sécuritaire du système TRANZIX, nous avons jugé intéressant de construire une application concrète qui exploite notre système. De plus, une deuxième application est proposée sur des bases conceptuellement différentes, montrant ainsi les vastes possibilités d'utilisation du système transactionnel TRANZIX.

5.2.1 Le contrôle des ressources physiques

Dans un premier temps, nous avons décidé de construire une application intranet capable de contrôler des périphériques, notamment des imprimantes. Cette application permet donc le contrôle de ressources physiques: des documents imprimés sur papier offerts contre un paiement électronique de la part de l'acheteur. Comme l'impression d'un document lors de l'utilisation de l'imprimante implique des dépenses d'encre et de papier, nous avons décidé de prendre en compte ces deux facteurs dans le calcul du prix à demander.

Il existe en effet plusieurs scénarios pouvant conduire à des coûts différents. Par exemple, il peut s'agir d'un très long document, avec beaucoup de texte et peu d'illustrations, ce qui implique beaucoup de pages et donc beaucoup de papier. Par ailleurs, le document peut être très court mais rempli d'images, ce qui implique

beaucoup d'encre. Comme il existe de nombreuses situations entre ces deux extrêmes, nous avons décidé de facturer les clients en fonction du volume, en octets, du document qu'ils veulent imprimer. Ceci implique une interaction intermédiaire entre le client et le «centre d'impression payante», afin de déterminer en-ligne, en fonction du document envoyé par le client, le coût de l'impression.

L'application consiste en une collection comprenant deux classes Java (`Emetteur.class` et `Recepteur.class`, la première installée du côté du vendeur et la deuxième du côté de l'acheteur) et deux scripts (`EMETTEUR.cgi` du côté du vendeur et `IMPRIMEUR` du côté de l'acheteur). Regardons comment elle fonctionne[3].

Une fois rendu à l'aide de son fureteur dans le «centre d'impression payante», le client est invité à démarrer l'application d'impression (`IMPRIMEUR`) et à cliquer sur le lien indiqué. À l'aide de l'interface (`interface.cgi`), ce lien déclenche l'application du vendeur (`EMETTEUR.cgi`) qui va contacter le client à l'aide d'une connexion TCP/IP. L'application d'impression du client attend d'être contactée par le vendeur; une fois le contact établi, elle demande au client le nom (avec le chemin complet) du fichier qu'il veut imprimer. Notons que le format du fichier n'est pas important, en autant que l'imprimante possède le pilote (*driver*) correspondant et sache comment l'imprimer. Le fichier est transmis au vendeur et la connexion est fermée.

Lorsque le fichier arrive sur le serveur intranet du vendeur, son volume est mesuré [par la partie vendeur de l'application] et un message est affiché dans le fureteur du client, lui indiquant le prix demandé pour l'impression. À ce stade ci, l'acheteur peut refuser le prix demandé, et quitter; son fichier sera alors effacé automatiquement du disque dur du «centre d'impression payante». Par contre, si le client choisit de poursuivre, il est invité à démarrer son module de facturation si cela n'a pas déjà été fait, et une transaction TRANZIX est initiée par le vendeur. Si la transaction est réussie,

[3] Une présentation en images est également disponible à l'Annexe I.

un message à cet effet précisant le nom de l'imprimante avec laquelle le document a été imprimé est indiqué dans le fureteur du client; l'acheteur peut alors aller chercher son document imprimé. Sinon, une page contenant des explications ainsi que les raisons possibles de l'échec est générée et affichée dans le fureteur de l'acheteur et celui-ci doit recommencer l'opération s'il désire toujours faire imprimer son document par ce «centre d'impression payante».

Comme nous avons déjà mentionné, ce processus peut prendre environ quelques dizaines de secondes ou moins, pour l'usager qui connaît déjà la procédure. C'est donc seulement quelques secondes supplémentaires qui s'ajoutent à l'impression d'un document, ce qui rend l'application tout à fait utilisable dans n'importe quel environnement de travail. Par ailleurs, il faut noter que le contrôle de périphériques se prête très bien à l'utilisation du système TRANZIX à l'intérieur d'un réseau local ou sur l'intranet d'une entreprise. D'autres périphériques peuvent aussi être contrôlés de cette façon, tels que des scanners, des tablettes traçantes, des portes, etc.

5.2.2 Le contrôle d'accès virtuel

Cette deuxième application diffère conceptuellement de la première en ce sens qu'elle offre le contrôle d'accès à des services virtuels: des informations contenues dans des pages virtuelles – sur le Web – sont offertes contre un paiement électronique. Le fonctionnement de cette application[4] ressemble à celui de l'application précédente à l'exception de l'étape intermédiaire d'affichage du prix, étape qui n'est plus nécessaire. Ainsi, une fois rendu dans la page «magasin» du vendeur, le client découvre une liste de services qu'il peut acheter, avec leurs prix correspondants, services tels que l'accès à une page d'informations en temps réel sur les cotations d'une bourse de valeurs. Le lien

[4] Une présentation en images est également disponible à l'Annexe II.

payant déclenche le démarrage du module de facturation sécuritaire du vendeur qui tente de contacter le logiciel de l'acheteur pour négocier la transaction.

Comme résultat, le client a accès immédiatement aux ressources demandées, sans nécessairement passer par des étapes intermédiaires qui retardent l'usager inutilement. L'échec de la transaction est traité comme dans le cas précédent. L'application permet de faire valoir les capacités de traitement des micropaiements du module de facturation, en offrant aux clients l'accès à des informations en échange de minuscules montants d'argent virtuel.

5.2.3 Autres applications possibles

En ce qui concerne l'accès à d'autres ressources logiques, les billets virtuels peuvent être remplacés par des jetons numériques. Des applications telles que celles décrites par [Hong et al., 1996], [Djeziri et al., 1997] ou [Zhou et Lopresti, 1997] pourraient alors constituer des exemples utiles avec lesquels TRANZIX pourrait être employé afin d'offrir un accès restreint à des informations précieuses extraites et archivées en format numérique.

D'autres types d'objets contrôlables peuvent aussi inclure l'accès physique à des endroits et locaux (portes, serrures, etc.). Pour contrôler l'accès à de tels objets, ainsi que la manière avec laquelle ils sont maniés et traités, notre système permet l'emploi de jetons numériques distribués de façon centralisée aux utilisateurs d'un intranet ou d'un extranet. Chaque jeton sert comme pièce justificative certifiée offrant un accès limité et conditionné à un objet prédéterminé. Les jetons sont standardisés et facilement personnalisables pour servir des ensembles prédéterminés d'objets ayant des détails d'accès spécifiés d'avance, tels que la date et l'heure d'utilisation, la quantité de ressources disponibles, etc.

Une autre application possible consiste à transiger des documents électroniques, indépendamment de leur contenu. La valeur d'une telle transaction n'est pas restreinte, étant donnée la granularité ajustable de notre système, qui permet d'effectuer des macro, mini et microtransactions. Un premier exemple de ce type d'application concerne l'accès à de gros documents (ou bases de données), tels que les livres. Très souvent, les usagers qui accèdent à de tels documents pour des informations ponctuelles ne veulent pas télécharger, et encore moins acheter, le document dans son entier. Un moyen pour résoudre ce problème est de permettre l'accès partiel au document (par chapitre, page ou paragraphe) ou à la base de données (permettant ainsi des consultations simples). Notre système permet d'effectuer un tel type de transaction en offrant la possibilité d'échanger des fractions arbitraires de documents, en fonction des choix effectués par leurs possesseurs. Les émetteurs, les banques et les marchands peuvent ainsi fragmenter tout document électronique de façon dynamique et vendre cette information à l'aide de TRANZIX, suivant un prix établi par le marché, en fonction de l'offre et de la demande. Par exemple, dans le cas de microtransactions, la valeur d'une quantité infime d'information est suffisamment petite pour les acheteurs (¼ cent, par exemple), et un nombre important de recherches (et donc d'achats) dans un tel document ou base de données peut leur coûter un faible montant (quelque cents, par exemple). Cependant, si le marchand reçoit un grand nombre de requêtes de recherche chaque jour – comme c'est le cas pour beaucoup de moteurs de recherche ou d'autres sites populaires – le montant d'argent total amassé à la fin d'une journée devient non-négligeable (par exemple, au prix mentionné plus haut 1,000,000 d'accès par jour dans la base de données pourraient générer plus de 75,000 $ par mois).

Notons que de telles quantités de transactions pourraient générer un trafic important surtout vers l'entité banque. TRANZIX permet de réduire les coûts substantiellement en offrant des options de paiement et de vérification hors-ligne. La vérification distribuée pourrait aussi être offerte, allégeant ainsi le travail de vérification du serveur central de l'émetteur. En fonction de la valeur d'une transaction donnée, les

marchands peuvent réduire de façon drastique leurs coûts en vérifiant les billets reçus par lots, à la fin de la journée, de la semaine ou du mois. Ces options permettent des réductions substantielles tant au niveau des coûts, qu'au niveau de la largeur de bande utilisée, rendant viables, d'un point de vue économique, les microtransactions.

Un autre exemple très utile concerne les ***transactions mixtes***, dans lesquelles différents types de valeurs sont échangés au cours d'une même transaction [Ureche et Plamondon, 1999b]. Un cas typique de transaction est l'échange de documents accompagnés d'un ou plusieurs billets virtuels, servant de paiement. Employant le PTEV, le système global TRANZIX offre la possibilité à toutes les entités transactionnelles d'utiliser leurs portefeuilles virtuels respectifs pour transiger de manière directe tout objet virtuel, permettant ainsi l'intégration des outils d'échange de documents électroniques et des outils de paiement numérique dans un seul instrument transactionnel.

Pour clarifier davantage ce type de transaction, examinons en détail un exemple hypothétique. Dans cet exemple, une compagnie possédant une archive virtuelle de cartes, «L'Archive de Cartes, inc.» – possiblement basée sur un système ressemblant à celui décrit par [Samet et Soffer, 1995] –, peut indexer, conserver, emmagasiner, et extraire certaines caractéristiques à partir des images numérisées de cartes géographiques. Supposons que «L'Archive de Cartes, inc.» ouvre son site Web offrant aux visiteurs des informations générales, mais aussi la possibilité de consulter, acheter ou échanger des données et informations. Ainsi, dans la zone transactionnelle du site, la compagnie pourrait décider d'offrir à ses clients, sur son extranet, des images numérisées ou des informations contenant des caractéristiques extraites à partir de telles images, et d'accepter en échange d'autres images, sous certaines conditions. La compagnie pourrait alors ouvrir un magasin virtuel utilisant un portefeuille virtuel TRANZIX, pouvant ainsi traiter les requêtes transactionnelles arrivant sur le réseau, lancées par les clients à partir d'un lien spécial dans la page du magasin (Fig. 5.2, étape

1). Ce lien appelle un script CGI – l'interface entre le serveur Web et le système TRANZIX – qui permet de déclencher l'ouverture du portefeuille virtuel du magasin[5] (Fig. 5.2, étape 2); le portefeuille virtuel du magasin établit alors une connexion avec le portefeuille de l'acheteur et lui envoie une requête de paiement correspondant à la transaction demandée (Fig. 5.2, étape 3).

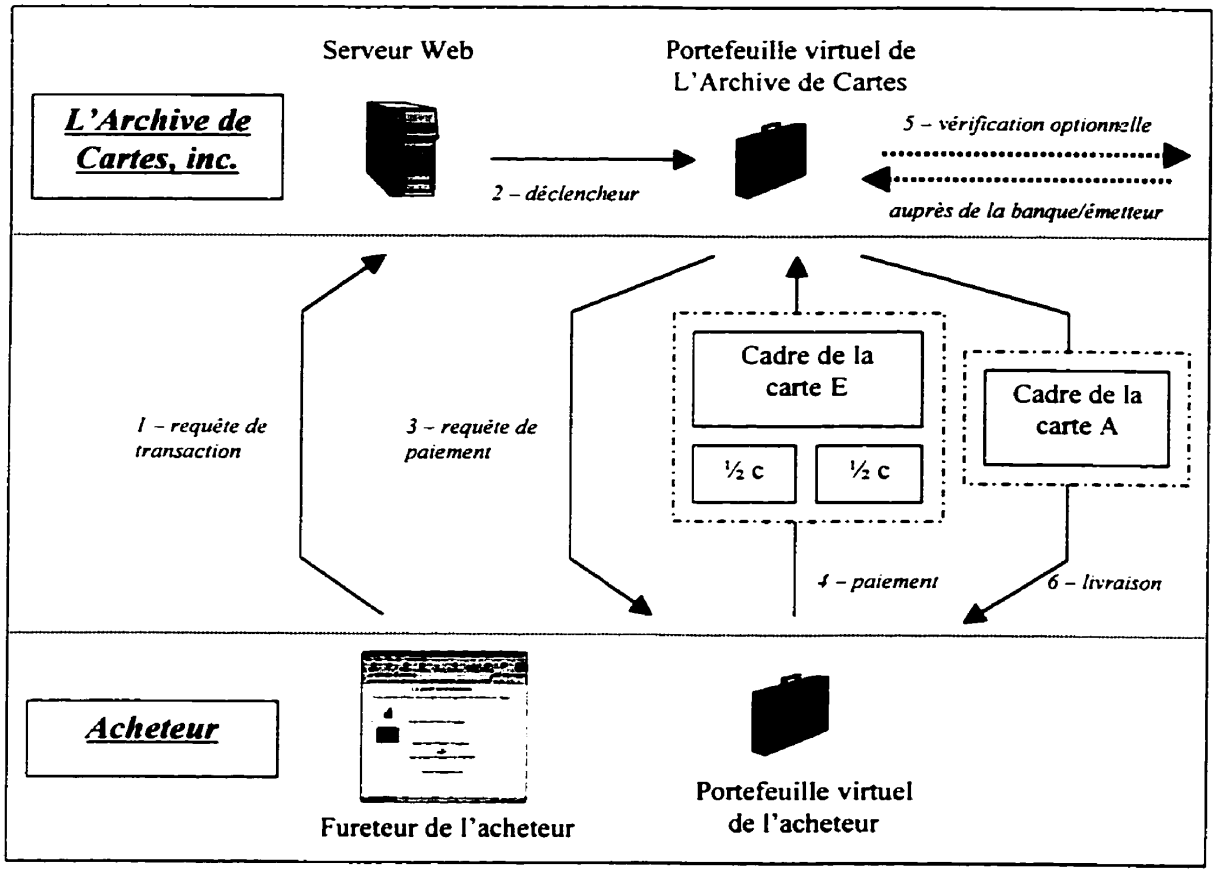

Figure 5.2 – *Un exemple de transaction mixte*

Supposons, pour les besoins de cet exemple, que les images numérisées des cartes sont divisibles et contiennent un numéro de série, un titre ou une description claire, ainsi qu'une signature numérique permettant d'authentifier ces informations. En

[5] C'est-à-dire le lancement du logiciel TRANZIX de la compagnie «L'Archive de Cartes, inc.».

employant ces éléments, «L'Archive de Cartes, inc.» peut décider qu'un cadre de la carte A, spécifié par le client et contenant $n \times m$ pixels, pourrait être:

1) acheté pour 2 ½ cents;
2) échangé pour un cadre prédéterminé contenant $p \times q$ pixels de la carte B ou C;
3) acheté pour 1 cent et un cadre prédéterminé contenant $r \times s$ pixels de la carte D, E ou F.

Une fois rendu dans le magasin virtuel, l'acheteur aura trois choix – affichés dans la zone transactionnel du site – tels que décrits plus haut. Il pourrait décider d'envoyer, par exemple, à l'aide de son portefeuille TRANZIX, le cadre demandé de la carte E accompagné de deux billets virtuels valant ½ cent chacun (Fig. 5.2, étape 4). Si le portefeuille virtuel du magasin a été configuré pour vérifier toutes les transactions en-ligne, ces trois éléments transactionnels seront tous envoyés à leur émetteur respectif pour vérification (Fig. 5.2, étape 5). La vérification de l'intégrité des messages transactionnels est réalisée localement. Le logiciel du magasin s'assure aussi que les conditions de l'échange ont été respectées; en employant les informations d'identification numériquement signées, le magasin pourra alors déterminer si le cadre de la carte demandée a été envoyé et si le montant correct a été inclus. Si la vérification est réussie, le portefeuille virtuel du magasin de la compagnie livre le cadre de la carte A au client (Fig. 5.2, étape 6). Tous ces échanges prennent place comme partie intégrante de la même transaction, utilisant les mêmes étapes du PTEV. De cette manière, non seulement les deux entités transactionnelles utilisent chacune un seul instrument logiciel, mais elles utilisent des instruments identiques, deux instances d'un même outil transactionnel intégré et multi-fonctionnel, permettant de simplifier le traitement efficace et la manipulation rapide des documents électroniques.

Nous venons de passer en revue quelques exemples où notre système pourrait s'avérer très utile. Même si cette liste d'exemples et d'applications n'est pas

exhaustive, la description de ces situations nous a permis de faire ressortir les principaux avantages du système TRANZIX, premier système électronique multi-fonctionnel de transport, transfert et d'échange numérique de valeurs.

5.3 Analyse des résultats expérimentaux

Nous allons présenter dans cette section une brève analyse des résultats obtenus lors des essais effectués avec le prototype expérimental du système TRANZIX. L'aspect primordial qui a été étudié est représenté par le temps requis pour effectuer différentes opérations, notamment le temps nécessaire pour la génération des clés cryptographiques et le temps de transaction, délai qui sera ressenti directement tant par les vendeurs que par les acheteurs.

5.3.1 La génération des clés cryptographiques

Lors du déploiement – ainsi que, éventuellement, lors des vérifications ultérieures –, en ne trouvant pas les clés numériques du client, le sous-module d'initialisation doit effectuer la génération des clés cryptographiques. Des informations d'identification (nom, adresse électronique) sont demandées alors à l'usager, ainsi que le choix de la longueur des clés. Un équilibre entre la sécurité et le temps de calcul doit être respecté afin d'assurer un fonctionnement adéquat. Avant de commencer la génération proprement dite, l'usager doit entrer une suite aléatoire – des caractères au hasard en mode texte ou simplement bouger le curseur en mode graphique. L'espace de temps mesuré entre les caractères ou les mouvements entrés permet de former une ***racine*** à partir de laquelle le logiciel génère des nombres aléatoires servant à la création

des clés. Le calcul proprement dit de la génération des clés est un travail long et complexe, surtout dans le cas de la cryptographie à clés publiques. De plus, le langage Java est la plupart du temps interprété, ce qui prend encore plus de temps. Des estimations empiriques montrent que les calculs cryptographiques sont environ 20 fois plus rapides si des modules compilés sont utilisés à la place des modules interprétés. Un compilateur Java juste-à-temps (JIT) peut aider d'une façon assez consistante, tel que démontré dans le Tableau 5.1 – qui rapporte les temps mesurés sur un ordinateur muni d'un microprocesseur Pentium P100 à 100 MHz.

Tableau 5.1 – *Tableau comparatif des temps de calcul des clés cryptographiques*

Longueur des clés	Java interprété	JIT	Java compilé
384 bits	780 secondes	97 secondes	38 secondes
512 bits	1281 secondes	152 secondes	56 secondes

En fonction de la longueur des clés choisie, ainsi que de la capacité et de la vitesse de l'ordinateur de l'usager, il faut s'attendre à des délais de une à vingt minutes (ou même plus) pour cette étape de génération des clés. Il est important de noter ici que cette période relativement longue d'attente ne sera plus répétée, à moins que l'usager ne perde ses clés ou ne décide de les changer. Par ailleurs, la permanente croissance de la vitesse de calcul des nouveaux microprocesseurs nous laisse entrevoir une baisse rapide de ces délais.

5.3.2 Le temps de transaction

Nous avons vu qu'une transaction peut prendre environ quelques dizaines de secondes ou moins, si le client connaît déjà la procédure. La partie la plus longue est le transfert de fonds, qui dépend grandement de la longueur des clés cryptographiques

utilisées. Le temps de transaction est le principal élément à considérer lors de l'analyse du système à l'aide du module-prototype, vu les implications qu'il peut avoir à différents niveaux de design. Comme les choix de design que nous avons effectués visent à rendre les calculs cryptographiques, la gestion interne du portefeuille et la gestion de la communication transparentes pour l'usager, seul le temps de transaction sort en évidence. Le temps de transaction peut être décomposé en plusieurs éléments:

- le temps de recherche et de sélection des billets nécessaires pour former le montant complet d'un paiement;
- le temps de signature (à l'envoi) ou de vérification de signature (à la réception) de chaque billet – temps qui s'additionnent s'il y a plusieurs billets dans un paiement;
- le temps de composition (à l'envoi) ou de décomposition (à la réception) des messages et des enveloppes virtuelles;
- le temps d'encryptage (à l'envoi) ou de décryptage (à la réception) des messages et des enveloppes virtuelles;
- le temps de transmission.

Nous rappelons qu'une enveloppe virtuelle peut contenir un ou plusieurs billets ou un reçu de paiement dûment signé. Comme une transaction n'est pas finie tant que la réponse finale du destinataire n'a pas été reçue, les composantes que nous venons d'énumérer doivent être comptées pour les deux partenaires transactionnels (donc dans les deux sens). De plus, comme pour tout autre logiciel, la vitesse de calcul du module de facturation sécuritaire TRANZIX sera évidemment influencée par le nombre d'autres applications utilisées en même temps sur l'ordinateur de l'usager.

Il est évident que si les quatre premières composantes relèvent de façon inhérente du module de facturation sécuritaire, le temps de transmission est une valeur qui échappe à tout contrôle et qui varie grandement non seulement d'un sous-réseau à

un autre, mais aussi suivant les heures d'une journée et en fonction de la congestion du réseau. Cette volatilité ne peut pas être contournée, même sur un intranet – sauf si la largeur de bande disponible est suffisamment importante pour pouvoir accommoder des crêtes (*peaks*) de trafic.

Nous estimons donc que l'analyse de ce facteur – le temps de transmission – sort du cadre de notre mandat et, par conséquent, pour simplifier notre analyse, nous allons lui donner une valeur fixe, en considérant toujours des conditions de transmission/réception idéales. Par ailleurs, les temps de recherche des billets, ainsi que les temps de composition/décomposition des messages peuvent être vus comme négligeables – nous allons les considérer comme des constantes de très faible valeur. Par contre, les deux autres composantes restantes du temps de transaction impliquent des calculs cryptographiques et donc du temps de calcul non-négligeable.

Analysons de plus près ce temps de calcul. Nous avons vu pourquoi ce temps est encore plus important lorsque Java entre en jeu. Nous savons aussi qu'il varie de le même sens que la longueur des clés cryptographiques et donc à la sécurité assurée. En effet, plus les clés utilisées sont longues, plus le niveau de sécurité est élevé, plus le temps de calcul s'accroît. Mais comment s'accroît-il ?

Nous avons effectué plusieurs tests et mesures empiriques, afin de faire ressortir cette variation. La Figure 5.3 montre la dépendance directe – ayant une croissance monotone – qui existe entre le temps total d'une transaction et la longueur des clés utilisées. Mentionnons que les transactions ont été, comme nous l'avons prévu, effectuées dans des conditions idéales, avec tous les temps de calcul et transmission – sauf les temps des calculs cryptographiques – stables et quasiment constants. Précisons aussi que les enveloppes virtuelles contenaient un seul billet numérique.

Notons l'aspect convexe de la courbe: en augmentant le niveau de sécurité, le temps de calcul est augmenté de façon très importante, ce qui implique un coût très grand pour passer à un niveau de sécurité supérieur sans une augmentation significative de la puissance et de la vitesse de calcul. Cependant, en doublant la longueur des clés, le temps augment d'un facteur confortablement inférieur à 100%.

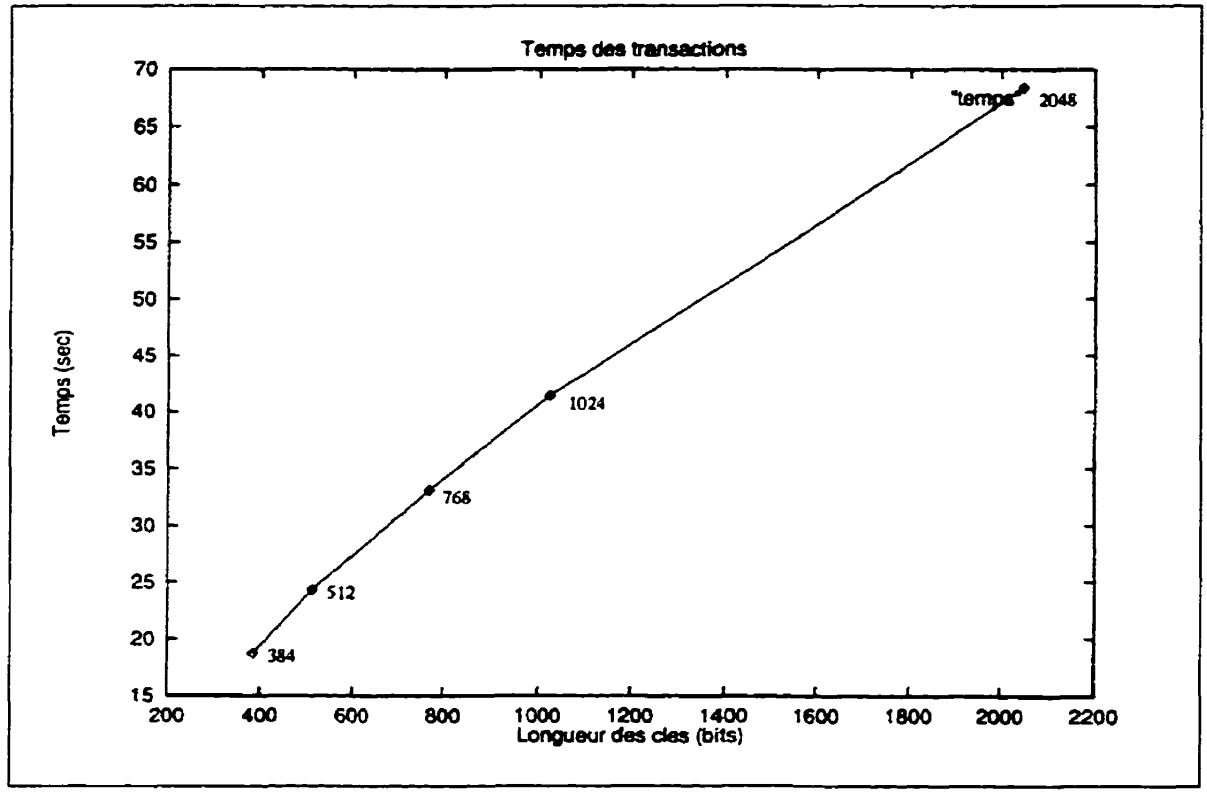

Figure 5.3 – *Le temps de transaction en fonction de la longueur des clés d'encryptage*

Ce qui ressort de façon très claire de ces résultats, c'est le besoin de trouver un équilibre, un compromis entre le niveau de sécurité désiré et la vitesse de calcul disponible – et donc le temps de transaction –, en jouant sur la longueur des clés cryptographiques. En même temps, notons qu'un temps total de transaction de moins de 20 secondes – équivalent ou même inférieur au temps nécessaire pour débiter une carte de crédit dans un supermarché ou pour télécharger une page Web avec quelques

illustrations ou *applets* – est, à notre avis, tout à fait acceptable et se compare bien avec les temps de transaction offerts par les autres systèmes de paiement électronique sur Internet commercialisés aujourd'hui.

5.3.3 Moyens d'optimisation

Le temps de transaction peut être optimisé encore plus pour le traitement des micropaiements qui peuvent nécessiter un niveau de sécurité moindre et donc utiliser des clés d'encryptage plus courtes. Pour des transactions plus importantes, des clés nettement plus longues peuvent être utilisées: même à plus de 60 secondes, avec des clés de plus de 2000 bits, il est difficile de voir d'autres moyens de paiement – incluant les cartes de crédit qui sont vérifiées à la caisse par téléphone – transférer des montants élevés, de l'ordre de plusieurs centaines ou même milliers de dollars, plus rapidement.

Il est intéressant de remarquer que l'originalité du système TRANZIX fait en sorte que les temps de transaction sont complètement indépendants du montant des billets transigés, donc de la valeur de la transaction; ceci rend très intéressante l'option de la ségrégation des clés: pour des valeurs importantes, un très haut niveau de sécurité pourra être offert, même si le temps de calcul sera plus long; pour des micropaiements, des clés très courtes pourront être utilisées, car même dans le cas d'une éventuelle fraude, seules des valeurs quasiment négligeables seront en jeu. En fait, même si le temps de transaction est indépendant de la valeur d'un échange numérique, dans la vraie vie, il sera probablement proportionnel à l'importance accordée à une transaction particulière.

Regardons quelques moyens pour optimiser les transferts de fonds et réduire encore plus le temps de transaction. Comme il ressort très clairement des paragraphes précédents, la réduction de la longueur des clés est extrêmement importante. Il faut donc

choisir le meilleur compromis entre la sécurité et la vitesse, en fonction de la valeur des transactions qu'on prévoit entreprendre.

Un autre moyen d'optimisation implique la réduction de la quantité d'information à encrypter/décrypter, en réduisant au strict minimum le nombre d'éléments inclus dans les enveloppes virtuelles, et notamment le nombre de billets numériques transigés. À cet égard, les vendeurs pourront demander à la banque émettrice d'émettre et de faire circuler des «billets sur mesure» ayant des valeurs nominales «personnalisées» en fonction de leurs besoins.

La banque peut aussi limiter la quantité d'information se trouvant dans l'historique des billets – quantité qui s'accroît au fil de transactions par lesquelles le billet passe, jusqu'à une certaine limite. Ainsi, en fixant une limite très basse sur le nombre de signatures attachées à un billet, et éventuellement un cycle très court d'expiration des billets, la banque peut réduire encore plus leur taille. En contrepartie elle devra faire face à un trafic plus élevé de billets à échanger. Encore une fois, ce paramètre peut être modulé en fonction de la valeur du billet.

5.3.4 La prévention des défaillances du serveur de la banque

Nous venons de voir que le système TRANZIX permet d'offrir des temps raisonnables de transaction, lorsque la communication entre deux ou plusieurs intervenants peut avoir lieu. Lorsque l'ordinateur de l'acheteur ou le serveur du vendeur sont bloqués, aucune transaction ne peut avoir lieu; mais une éventuelle défaillance du serveur de la banque pourrait avoir des conséquences beaucoup plus importantes. En effet, dans ce cas les clients ne pourront plus avoir accès à leurs fonds ou aux autres valeurs déposées à la banque; en même temps, les vendeurs ne pourront plus vérifier les paiements reçus, ni consulter le «babillard électronique» de la banque qui permet la

vérification distribuée des paiements. Il est donc évident qu'il est absolument nécessaire pour toutes les banques utilisant le système de prendre des mesures de prévention des défaillances, surtout au niveau de leurs équipements matériels.

De telles défaillances peuvent avoir lieu non seulement lorsqu'il y a une panne matérielle, mais aussi lorsque le nombre de transactions dépasse la capacité maximale de traitement de la banque. Regardons quelques modalités de prévention des défaillances [Martin, 1994] des serveurs de l'entité banque, en faisant abstraction des facteurs externes, comme les problèmes dus aux lignes de communications. Pour prévenir les éventuelles défaillances nous suggérons trois alternatives, soit:

1) la duplication de l'équipement (système *duplex*). Au niveau de base, chaque serveur de la banque disposera d'une plate-forme miroir avec tous les périphériques afférents, qui devra prendre la charge en cas de panne du serveur principal;
2) des procédures de recul (*fallback*). Une défaillance dans une composante du système ne représente pas toujours une défaillance du système en entier. En utilisant une hiérarchie de procédures de recul, une défaillance totale pourrait être évitée. Ainsi, par exemple, le serveur de la banque pourrait laisser tomber toutes les demandes de connexion, ou, au niveau hiérarchique inférieur, laisser tomber les connexions en attente, et finir seulement les transactions qui se trouvent déjà dans le système, etc.;
3) des procédures d'évitement (*bypass*). Avec cette stratégie, certaines transactions simples pourraient toujours être effectuées, même si une ou plusieurs composantes du système sont tombées en panne. Par exemple, les usagers pourraient obtenir le solde de leur compte, même s'il est impossible d'effectuer des retraits ou des dépôts.

Il s'agit donc d'effectuer une mise à l'échelle des systèmes informatiques de l'entité banque – en terme de nombre d'ordinateurs, de leur puissance, de leur capacité de stockage, des procédures de prévention des défaillances, de la capacité de communication et la largeur de bande (*bandwidth*) – afin de s'assurer que la qualité du service ne diminue pas lorsque le nombre de transactions augmente ou dans le cas d'une défaillance. En ce qui concerne la capacité maximale de traitement, une telle mise à l'échelle pourrait être effectuée par étapes, en fonction du nombre de clients qui ont adhéré au système et de leur niveau d'activité transactionnelle. Notons qu'une grande partie de ces mesures sont déjà en place dans la plupart des institutions financières, ce qui implique qu'il n'y aura pas de dépenses supplémentaires à cet effet.

5.4 Autres caractéristiques du système

Regardons finalement quelques autres aspects qui méritent d'être mentionnés avant de conclure ce chapitre. Tout d'abord, pour ce qui est de la vérification en-ligne de l'authenticité et de la validité des billets, mentionnons le fait que le système utilise le raisonnement logique par défaut. Le calcul de vérification est simple et direct:

Pour tout numéro de série N et usager U:
(A) si le billet qui vient d'arriver, ayant le numéro de série N, a été *déjà* déposé - donc le billet est *faux* -, ET
(B) si le fait que l'usager U vient de transmettre le billet N est *consistent* avec les autres informations disponibles, alors nous pouvons conclure que
(C) le billet ayant le numéro de série N a été falsifié par l'usager U.

La première proposition est prouvable, car l'émetteur possède la liste des dépôts, contenant le numéro de série de chaque billet déjà déposé, qu'il soit encaissé ou non. S'il est consistent de supposer la proposition B, alors nous pouvons conclure C. Ce type de logique ne peut pas, toutefois, être appliqué dans le cadre des paiements hors-ligne, car un billet falsifié par copiage peut passer par plusieurs intermédiaires avant de se retrouver à la banque, et le dernier propriétaire du billet (celui qui le dépose à la banque) n'est pas nécessairement le fraudeur. Nous avons montré en détail dans la section 4.4 du chapitre précédent comment la vérification des transactions hors-ligne peut être assurée.

Dans un contexte différent, mentionnons le fait que TRANZIX offre aux magasins virtuels un très court délai d'encaissement. Le système offre en même temps un niveau raisonnable d'anonymat, pouvant ainsi répondre en même temps aux besoins de sécurité, de confidentialité et de respect de la vie privée des consommateurs, d'une part et, d'une autre part, aux besoins des gouvernements pour lutter contre le crime organisé. Par défaut, aucun paiement n'est effectué automatiquement, sans consulter l'usager; aucune facturation ou transfert de fonds n'est acceptée automatiquement non plus et tous seront vérifiés en-ligne auprès de la banque. Le mode de communication est toujours, dans la mesure du possible, en-ligne et le port de communication est toujours le port 4949. Pour l'«utilisateur moyen» ces options assureront un fonctionnement normal. Pour les «utilisateurs avancés» par contre, certaines options pourront être changées. Par exemple, si dans une entreprise le lien au réseau Internet est assuré par un serveur intermédiaire *proxy*, tous les utilisateurs vont se retrouver sur le même ordinateur pour communiquer avec l'extérieur et il sera nécessaire de changer le numéro de port de communication afin de les distinguer les uns des autres.

Lors de l'implantation du moteur transactionnel, un effort très important a été consacré à la réalisation du protocole transactionnel de facturation, protocole très strict et sévère, afin de réduire au maximum les risques de pénétration malicieuse. Ainsi,

comme tout message incorrect ou «hors-séquence» génère une réponse de fermeture et la fin de la communication. il est très difficile de se rendre compte, lorsqu'il y a une erreur, à quel niveau elle se trouve. Aucune modification n'a été effectuée à ce niveau pour alléger le protocole, justement pour ne pas diminuer ou même compromettre ce qui a été déjà acquis.

Évidemment, dans une version commerciale, des améliorations pourront éventuellement être apportées. Comme nous l'avons déjà mentionné, l'algorithme qui permet de choisir les billets dans le portefeuille, afin de former le montant exact d'un paiement – si possible –, n'est pas optimisé; en l'optimisant, il pourrait, par exemple, essayer de minimiser le nombre de billets choisis. Cependant, il faudra se demander quel sera le coût de cette optimisation et étudier si une telle recherche optimisée aura finalement un impact négatif en prenant plus de temps que l'on sauve en envoyant moins de billets.

5.5 Conclusion

Nous venons de survoler le module de facturation sécuritaire TRANZIX, prototype squelettique et première implantation du système électronique de transfert numérique de valeurs. Après avoir exposé le contexte dans lequel la réalisation de ce prototype s'inscrit, nous avons regardé de près la structure interne du logiciel et celle de ses composantes internes et externes. Nous avons vu comment sont assignées les différentes tâches et comment les protocoles régissent les interactions entre deux entités transactionnelles. Deux applications concrètes du logiciel ont été développées et décrites – d'une part, le contrôle des ressources physiques et, d'autre part, le contrôle

des services virtuels, applications concrétisées par le contrôle des périphériques dans un réseau intranet, et le contrôle des accès dans un site Web, respectivement.

Enfin, nous avons analysé différents aspects portant sur les temps de génération des clés cryptographiques et sur le temps de transaction. Nous avons ainsi démontré la nécessité d'arriver à un compromis entre le niveau de sécurité désiré et la vitesse de calcul disponible, en tenant compte des applications concrètes et du contexte dans lequel le système transactionnel sera utilisé. Des moyens d'optimisation ont été par la suite proposés. Pour conclure, quelques autres aspects ont été brièvement discutés.

CHAPITRE 6

IMPACTS SOCIO-ÉCONOMIQUES POTENTIELS

L'économie mondiale, à l'époque de la révolution informationnelle et de l'avènement en force du commerce électronique, vient d'entrer dans une période de changements fondamentaux sans précédent. Ces transformations changeront non seulement la façon dont nous effectuerons des achats, mais en même temps ils renverseront aussi la nature de la compétition dans le monde économique. Cependant, plusieurs aspects restent encore à résoudre et des désaccords de longue durée sur les standards, sur les systèmes d'opération ou sur les infrastructures à adopter menacent les investissements à long terme. Par ailleurs, des technologies très prometteuses, comme la cryptographie à clés publiques et la biométrie, permettent d'accroître la confiance du public dans le commerce électronique.

Après avoir analysé l'état de l'art dans le domaine du paiement numérique sur Internet et après avoir introduit un nouveau système transactionnel, nous avons jugé utile de discuter, au meilleur de nos connaissances, des éventuels impacts que TRANZIX et d'autres systèmes semblables, pourraient avoir sur certains aspects de l'économie et de la société dans le futur. Si notre système généralise plusieurs notions et concepts présents dans les systèmes actuels de paiement électronique, il n'en reste pas

moins, à sa base, un outil financier, même si l'argent n'est plus le seul moyen permettant d'effectuer des paiements – des documents électroniques pouvant, par exemple, constituer une forme de paiement, en échange d'autres documents.

6.1 Le transfert de valeurs et l'argent numérique

Dans la foule d'éléments et d'applications qui forment le concept de commerce électronique, le système TRANZIX porte sur la sécurité des transactions et, plus spécifiquement encore, sur le transport de valeurs. Si la certification, le transport, le transfert et l'échange de documents électroniques ne pose pas de problèmes majeurs aux niveaux décisionnels ou stratégiques, la situation est complètement différente pour ce qui est de l'argent numérique.

En effet, une fois certifié en employant des moyens efficaces et non-contrefaisables, un document électronique peut être véhiculé, à l'aide de protocoles sécuritaires, en toute quiétude de sa source jusqu'à sa destination. Des moyens pour assurer la propriété intellectuelle, qui restent encore à développer[1], sont parmi les seules questions qui sont toujours en suspens. Par contre, l'utilisation de l'argent comme valeur transigée numériquement amène un nombre considérable de complications de nature décisionnelle, stratégique et parfois même de nature politique. C'est pour ces raisons que nous allons nous concentrer dans les pages qui suivent sur le côté monétique du transfert de valeurs et nous allons soulever plusieurs questions portant sur différents aspects concrets des éventuelles implantations à large échelle des systèmes monétiques numériques.

[1] À ce jour, des systèmes tels que ceux employant des moyens de «filigranage» (*watermarking*) électronique ont été proposés pour certaines applications, telles que les images numériques.

Au fil des siècles, une des premières façons de représenter la valeur comme élément économique a été d'utiliser la valeur intrinsèque d'un bien. L'histoire nous montre plusieurs moyens originaux de représenter la valeur, en partant du troc, en passant par les coquilles et les pièces d'or et d'argent, pour finalement arriver aux billets de papier et aux cartes de plastique. Il n'est pas difficile de se rendre compte du fait que plus on s'éloigne de l'époque du troc, moins la valeur économique de l'unité d'échange est représentée directement par sa valeur intrinsèque. De plus, depuis une vingtaine d'années, elle n'est plus représentée – et garantie – par les réserves en or des banques centrales émettrices. De façon générale, la valeur d'une devise, qu'elle soit représentée par une pièce de monnaie, par un billet de papier ou autre, n'est pas représentée aujourd'hui de façon précise. En effet, la valeur d'une devise dépend aujourd'hui d'une multitude de facteurs macro-économiques, tels que le taux de croissance de la masse monétaire, le taux d'inflation ou le déficit commercial et budgétaire. La valeur est donc garantie par la quantité de biens et services produits de façon globale, dans le système économique en entier.

L'argent n'est qu'un intermédiaire servant à l'échange de valeurs. En tant qu'instrument économique, il remplit trois fonctions de base dans la société:

- il sert de moyen pour compter des objets ayant une valeur, ou d'unité comptable. Par exemple, une imprimante vaut X dollars;
- il constitue un moyen commode d'emmagasiner des valeurs pour un usage ultérieur. Par exemple, la possession de l'imprimante est remplacée par la possession de Y billets représentant X dollars qui pourront être dépensés plus tard pour acheter une quantité Z de disquettes;
- il est un moyen d'échange universel. Par exemple, au lieu de troquer l'imprimante pour des disquettes, les disquettes peuvent être achetées par l'intermédiaire d'une partie de l'argent obtenu sur l'imprimante.

Nous croyons que ces fonctions sont des conditions essentielles, nécessaires mais pas toujours suffisantes, pour la survie à long terme de tout système monétaire. Pour remplir ces fonctions, tout système doit également satisfaire aux exigences déjà décrites dans le Chapitre 4, sous-section 4.4.2. Ainsi, un tel système pourrait devenir, dans des conditions favorables, un système monétaire généralement accepté par la société.

Dans le commerce électronique, parmi les systèmes de paiement électronique, seuls les systèmes employant des pièces ou billets numériques introduisent une nouvelle forme d'argent, l'argent virtuel; tous les autres systèmes, incluant ceux basés sur les cartes de crédit, ne représentent que des nouvelles modalités de transfert de fonds. Mais quelles seront les implications potentielles d'une éventuelle acceptation à large échelle des nouvelles formes de représentation monétique ? Quelles seront leurs conséquences directes ?

6.2 Vers une nouvelle micro-économie potentielle

Nous allons nous interroger dans cette section sur plusieurs points concernant le transfert numérique de valeurs, et plus particulièrement, sur les aspects monétiques reliées au système transactionnel proposé dans cet ouvrage de même qu'aux autres systèmes semblables. Concrètement, nous allons considérer le concept général suivant: l'implantation à grande échelle, dans un future proche, d'un système électronique de transfert numérique de valeurs, tel que TRANZIX, afin de former une communauté micro-économique virtuelle basée sur le commerce électronique et l'échange sécuritaire de valeurs; ainsi, chaque groupe d'entités peut devenir lui-même un sous-système transactionnel dans une «sous-communauté» micro-économique. Dans ce

contexte, quels seront les impacts sur les différents intervenants, comment les entités transactionnelles seront-elles affectées ?

6.2.1 Les impacts potentiels sur les différents intervenants

En fonction du niveau de déploiement, à une échelle locale, provinciale, nationale ou internationale, les impacts potentiels d'un ensemble de systèmes de paiement électronique seront évidemment différents. Ainsi, pour les acheteurs, un tel système offre la possibilité de magasiner partout à travers la planète, donnant un choix de produits et services plus vaste et des prix moins dispendieux. Le consommateur aura ainsi la commodité de magasiner facilement, de payer ses factures, d'effectuer toutes ses transactions de façon rapide et sécuritaire, tout en restant chez lui, et pour un coût très compétitif. De plus, un système comme TRANZIX, permettant le transfert sécuritaire d'autres valeurs à part l'argent, permettra un choix encore plus varié de transactions à distance, généralisant les opérations de paiement, d'acquittement de factures et d'échanges électroniques en général.

Un autre aspect potentiellement très important sera l'accès direct des consommateurs aux marchés financiers, aspect qui aura sans doute un impact majeur. Avec la baisse des frais et des tarifs et la commodité offerte par les nouveaux logiciels utilisant l'Internet, changer des dollars virtuels en yens virtuels sera tout aussi facile et immédiat que n'importe quelle autre transaction[2]. Or, des vagues de consommateurs achetant ou vendant une devise – ou toute autre marchandise transigée sur un marché financier – pourraient générer une volatilité sans précédent sur les marchés boursiers et d'échange.

---

[2] Les consommateurs peuvent effectuer déjà, depuis quelque temps, des transactions boursières par Internet, à faible coût, par l'intermédiaire des courtiers à escompte.

Pour les vendeurs s'ouvrent de vastes nouveaux marchés, donnant à leurs produits et services une portée mondiale [Kambil, 1997]. Avec une clientèle tellement importante, les ventes augmenteront de façon substantielle, créant ainsi une demande renforcée qui se propagera aux autres niveaux de l'économie: de nouveaux emplois pourraient être crées, pour satisfaire cette poussée de la demande. À part les hautes technologies, un des premiers secteurs avantagés sera, à notre avis, celui des transports, et en particulier celui du courrier rapide, qui devra prendre en charge le transport physique des biens commandés et achetés à distance.

Si aujourd'hui un marchand qui offre un site transactionnel détient un avantage concurrentiel sur ses compétiteurs qui ne sont pas encore branchés, dans quelques années cet avantage n'existera plus, car une grande majorité de vendeurs seront fort probablement déjà branchés. Plus encore, ceux qui ne seront pas encore branchés seront dans une situation de net désavantage concurrentiel. En même temps, l'«entreprise à domicile» connaîtra, fort probablement, un essor sans précédent. En effet, l'Internet permet d'uniformiser les opportunités de tous, le site Web d'un petit commerçant pouvant avoir une qualité ou une popularité supérieure à celui d'une grande compagnie multinationale. Ceci permettra une meilleure distribution des ventes et des revenus, le petit détaillant pouvant ouvrir rapidement et faire fonctionner facilement un service de commandes par la poste dans son sous-sol.

Parmi les bénéfices de la concurrence acerbe qui suivra, il y a évidemment des prix nettement moins dispendieux. Par exemple, les coûts de location d'un magasin virtuel ainsi que le personnel restreint requis pour son fonctionnement et pour son entretien réduiront encore plus les dépenses des vendeurs. De plus, l'emplacement physique de l'entreprise sera quasiment transparent pour le consommateur; par exemple, une entreprise asiatique pourra offrir ses services sur un même serveur qu'une compagnie nord-américaine ou européenne, mais avec des coûts de production nettement inférieurs. Cette transparence amènera cependant des difficultés pour les

gouvernements nationaux, non seulement au niveau du cadre législatif et juridique du commerce électronique, mais aussi au niveau de l'imposition et de la taxation de cette activité économique. En effet, il est difficile à préciser aujourd'hui quel gouvernement percevra les taxes de vente sur une marchandise produite au Québec, vendue par un marchand allemand ayant son magasin virtuel sur un serveur situé physiquement aux États-Unis. D'autres effets négatifs apparaîtront sans doute. Par exemple, entre autres, les magasins virtuels de l'économie numérique auront besoin de beaucoup moins de personnel, ce qui ce qui engendrera inévitablement du chômage.

Les modèles de vente et de marketing évoluent aussi, tout comme les modèles d'affaires. Si le modèle traditionnel de vente de «l'utilisateur payeur» implique l'échange d'un paiement de l'acheteur contre des biens et des services offerts par le vendeur, ce model n'est certainement pas le seul. Un modèle utilisé largement dans la télédiffusion est déjà utilisé avec succès sur Internet. Il s'agit de la publicité présente sur les sites des vendeurs qui remplace les paiements des clients comme source de revenus par les paiements d'autres marchands. Ce modèle est très bien intégré avec les sites de nouvelles, dans lesquelles les visiteurs lisent sans rien acheter.

En d'autres cas, les vendeurs peuvent aussi laisser l'accès gratuit à leurs catalogues, faisant alors leur profit sur les ventes réelles. Notons le fait qu'un vendeur pourrait aussi utiliser dans de tels cas un outil transactionnel comme le système de transfert généralisé de valeur TRANZIX, étant donnée sa grande flexibilité au niveau des types de valeurs qu'il peut transférer et, implicitement, des paiements qu'il peut réaliser. Les vendeurs pourraient alors ne plus effectuer directement des microtransactions avec les acheteurs mais transiger plutôt de plus gros paiements avec les distributeurs de publicité, les compagnies publicitaires, ou directement avec les autres marchands, dans un modèle transactionnel interentreprises. De plus, TRANZIX permet d'effectuer d'autres types de transferts, incluant les échanges des contrats, des ordres, des factures, etc.

Enfin, les banques se retrouveront, comme les autres entreprises et institutions, sur la voie du développement accéléré [McChesney, 1997]. Un système économique basé sur l'argent électronique pourrait, à notre avis, leur permettre une prospérité encore plus élevée que celle d'aujourd'hui. En effet, avec des réductions dramatiques des coûts des transactions, assorties d'un accroissement potentiellement massif de la clientèle dans un marché unique et mondial, les profits nets pourraient monter de façon substantielle. La concurrence qui surgit déjà partout entraînera, fort probablement, un plus grand nombre de fusions et de consolidations d'entreprises et une baisse générale des coûts pour tous les intervenants.

La question des prix et des coûts est devenue aujourd'hui un aspect économique essentiel. En regardant les coûts de traitement d'une transaction dans la Figure 6.1, nous pouvons nous rendre facilement compte que l'argent électronique défie toute concurrence. De plus, avec des économies d'échelle, basées sur des grands volumes transactionnels, assorties du profit offert par l'intérêt généré par les réserves qui supporteront habituellement les billets virtuels[3], les émetteurs réduiront encore plus ces coûts, pour les ramener – de façon asymptotique – de plus en plus près de zéro. Ceci donnera une raison d'être économique aux microtransactions qui, à leur tour, ouvriront de nouvelles possibilités et opportunités pour la créativité humaine. Les grandes compagnies pourront ainsi explorer des niches qui étaient auparavant trop petites pour être profitables, tandis que les PME pourront augmenter leur portée pour atteindre les marchés mondiaux.

---

[3] – le ***seigneuriage***: différence entre le prix de vente d'une monnaie et le coût d'émission. De plus, pour émettre un dollar virtuel, un émetteur doit détenir, en fonction du type de couverture choisie, un dollar [ou moins] réel – ou de l'or, d'autres valeurs, etc.; ce dollar gagne de l'intérêt avec le temps. Ainsi, par exemple, la banque centrale américaine, **The US Federal Reserve**, gagne annuellement environ 20 milliards de dollars US sur ses 400 milliards de dollars US en circulation.

En même temps, les banques auront à répondre à une question plus difficile: quel système adopter ? En adopter plusieurs, pourra leur coûter cher, mais ils ne pourront probablement pas se permettre de ne pas entrer dans cette nouvelle forme de commerce électronique. Tout comme pour les autres instruments financiers, un ensemble de solutions – qui répondent chacune à des besoins spécifiques – aura, à notre avis, des fortes chances d'être adopté. D'autres décisions difficiles devront être prises par les banques, comme nous allons le voir dans les sous-sections suivantes, surtout pour celles qui assumeront le rôle d'émetteur.

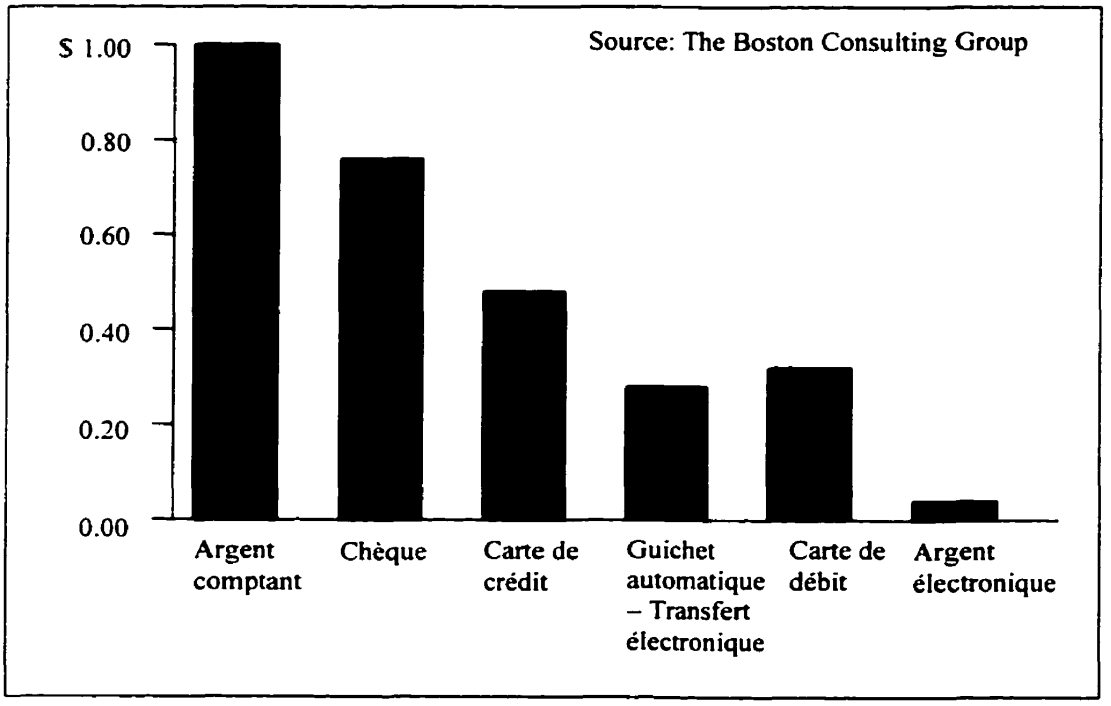

Figure 6.1 – *Les coûts de transaction en fonction du mode de paiement*

Les nouvelles technologies de paiement électronique introduisent plusieurs nouveaux moyens pour distribuer les risques, les responsabilités et les coûts entre les intervenants impliqués dans une transaction [Maat, 1997]. Il faudra s'attendre toutefois à ce qu'un certain temps s'écoule avant que les habitudes des consommateurs et les

réglementations juridiques – qui évoluent beaucoup plus lentement que les hautes technologies – changent. Le succès d'un système transactionnel sera aussi déterminé par la facilité avec laquelle les consommateurs pourront s'y joindre et par les opportunités d'achat qu'ils auront, opportunités déterminées par le nombre et par la qualité des vendeurs disposés à offrir leurs biens et services contre cette nouvelle forme de paiement. Pour un succès rapide, les émetteurs qui adopteront un nouveau système électronique de paiement devront s'assurer que leurs clients sauront où dépenser leur argent. Ils devront donc encourager –même subventionner – des vendeurs, afin de les convaincre des avantages du nouveau système et des opportunités qui découleront de son utilisation.

6.2.2 Types d'émission

6.2.2.1 Émission centralisée

Si l'émission de certificats pour signer et ainsi authentifier des documents électroniques peut être effectuée par tout usager d'un système de transfert de valeurs, le problème se complique lorsqu'il s'agit d'argent numérique. En effet, nous devons nous poser la question suivante: quel type d'émission de monnaie virtuelle est le plus indiqué, l'émission privée ou l'émission centralisée ? Qui pourra émettre de l'argent virtuel ayant un cours légal ?

En ce qui concerne ce dernier aspect, si l'émission de la RM est basée directement et complètement sur une devise réelle ayant déjà cours légal, si l'émetteur est une banque centrale ou autre organisme gouvernemental et si des dispositions législatives claires en ce sens ont été prises, cette RM pourrait alors avoir cours légal pour tous les intervenants ayant les moyens techniques de l'utiliser. Par ailleurs, si une RM est généralement acceptée à large échelle, même si l'émetteur n'est pas une banque

centrale, elle pourrait avoir un statut équivalent à une devise ayant cours légal, surtout si des organismes gouvernementaux l'acceptent comme moyen de paiement.

Nous proposons, à court terme, une approche centralisée, impliquant la participation d'un nombre limité d'émetteurs. L'avantage de cette approche est immédiat: les consommateurs pourront avoir une idée claire de la confiance qu'ils peuvent avoir dans l'émetteur central et dans la valeur que la RM émise détient. De cette manière, le niveau de confiance dans un tel système pourrait augmenter rapidement pour atteindre une masse critique permettant une adoption à grande échelle. Cet effet pourrait être amplifié davantage en cooptant une institution bancaire bien connue, de renom, un organisme gouvernemental ou une banque centrale, organismes et institutions qui pourront augmenter encore plus le niveau de confiance dans le nouveau système transactionnel.

6.2.2.2 Émetteurs multiples et monnaie privée

Dans notre système symétrique, un élément innovateur très utile est la capacité de chaque entité de changer ou même de combiner les rôles; ainsi, par exemple, un usager pourrait théoriquement créer ses propres billets numériques privés, pourrait les vendre et en acheter d'autres, devenant ainsi émetteur, vendeur et acheteur. L'utilité de cette caractéristique est évidente: elle permet à tous les usagers non seulement de vendre et d'acheter en même temps en utilisant le même logiciel, mais aussi d'émettre et de certifier leurs propres documents électroniques ou billets numériques, permettant ainsi de créer une micro-économie numérique localisée.

Après avoir obtenu un niveau suffisamment élevé de confiance, basé sur une émission centralisée, un système comme TRANZIX pourrait permettre de passer, à long terme, à l'émission privée, donnant ainsi la possibilité à tous ses usagers d'émettre non seulement des certificats authentifiant des documents électroniques mais aussi des billets

numériques ayant une valeur monétaire. Ces valeurs ressembleront plutôt à des jetons ou à des coupons personnalisés acceptés [presque] seulement auprès de leurs émetteurs, un peu comme les coupons des supermarchés. Toutefois, une telle approche pourrait donner une liberté économique sans précédent, renforcée davantage, par une éventuelle déréglementation et démonopolisation des émissions monétaires.

Aujourd'hui, à l'heure de la mondialisation, le succès escomptée de la monnaie commune européenne, l'euro, laisse entrevoir un regroupement autour de quelques devises à grande circulation – le dollar américain, l'euro et le yen japonais. Cependant, des monnaies privées pourraient toujours trouver une niche dans une économie de plus en plus compartimentée [Lépinay et Audet, 1999].

Un autre aspect concernant les monnaies privées est celui des assurances. Que se passe-t-il si, lors d'une crise économique, l'émetteur fait faillite ? Les billets virtuels en circulation devront-ils être assurés ? Nous estimons que non: l'argent virtuel n'est pas un dépôt traditionnel, assurable comme les dépôts assurés par la **Société d'assurance-dépôts du Canada**. Tout comme l'argent réel, les billets virtuels, qui changent seulement de forme pour accéder à l'espace virtuel, n'ont pas beaucoup de raisons pour devenir assurables, ils appartiennent au porteur. Toutefois, il y a des arguments contre cette position. Ainsi, au début de «l'âge des monnaies numériques», il est probable que les émissions d'argent virtuel seront couvertes par d'autres valeurs, telles que les devises réelles. Or, ces valeurs de couverture pourront être assurables; de plus, elles gagneront de l'intérêt, qui en partie pourra couvrir les coûts des transactions ou pourra, en partie, être redistribué aux utilisateurs du système sous forme d'intérêt ou d'assurances sur les billets virtuels en circulation. Cette décision sera probablement prise suite à la concurrence que les émetteurs se feront pour attirer des nouveaux clients. De cette façon, non seulement les consommateurs pourront gagner de l'intérêt sur l'argent qu'ils détiennent dans leurs portefeuilles virtuels (sur leurs disques durs), mais ils auront aussi accès à des services bancaires gratuits ou à des prix très compétitifs.

Dans le court terme, le désavantage des monnaies privées est évident. Si chaque usager émet ses propres billets, il y aura après peu de temps une «économie des coupons» à la place d'une monnaie liquide et mondialement reconnue. Ces monnaies privées seront, fort probablement, difficilement échangeables; il sera aussi difficile de les évaluer, de leur donner une valeur relative, ce qui entraînera une baisse générale de confiance de la part des consommateurs, qui essaieront de se «réfugier» dans des monnaies «officielles», plus connues et plus sûres. Même si le nombre d'émetteurs est relativement restreint, il est possible de se retrouver dans une situation similaire avec celle connue au Canada et aux États-Unis au siècle dernier, lorsque chaque état américain ou banque privée pouvait émettre ses propres billets. Comme il fallait effectuer des échanges d'une devise à une autre, impliquant donc des coûts additionnels et des commissions, les billets étaient seulement acceptés avec un escompte – par exemple 19 dollars pour un billet de 20 $. Cependant, nous pouvons argumenter ici qu'aujourd'hui, avec une grande puissance de calcul disponible à un coût dérisoire, il sera beaucoup plus facile d'échanger automatiquement une monnaie virtuelle privée contre une autre, en couvrant de façon réciproque ou en «troquant» les coûts d'échange les uns contre les autres.

Notre opinion sur ce point est que la question des monnaies privées sera ramenée à une question de confiance que les consommateurs montreront envers une devise numérique donnée. Plus la réputation d'un émetteur sera reconnue, plus sa devise virtuelle aura de la valeur, ce qui entraînera plus de consommateurs à l'acheter ou même à l'utiliser comme «refuge» dans le cas d'une panique ou d'une crise.

6.2.3 Types de couverture

Toujours du côté des émetteurs, un autre aspect important concerne les moyens de garantir les valeurs représentées numériquement. Comment garantir l'argent

virtuel émis ? Les nouvelles monnaies seront-elles flottantes ou seront-elles couvertes par des devises réelles (*peg* ou *swap* 1 à 1) ?

Nous envisageons plusieurs types de couverture permettant de garantir ou de soutenir la valeur d'une représentation monétaire. Ainsi, une monnaie virtuelle qui n'est pas basée sur des valeurs généralement acceptées n'aura pas, à notre avis, de grandes chances de succès.

Pour commencer à utiliser de l'argent numérique, un peu comme dans le monde réel, il s'agit d'échanger une devise réelle contre une devise virtuelle. À moins que cette dernière ne soit garantie par la confiance que les consommateurs peuvent avoir dans l'institution émettrice, elle doit être couverte par d'autres valeurs, que ce soit des produits ou des services, d'autres devises, etc. Ainsi, un prix de vente (ou un taux de change) pourrait être fixé pour la nouvelle monnaie virtuelle, permettant d'estimer ainsi sa valeur.

Si l'émetteur choisit de baser chaque unité de sa RM sur une unité d'une devise réelle – déposée en bonne et due forme dans ses propres coffres ou auprès d'un tiers – en les échangeant unité pour unité, il opte alors pour la couverture complète (*swap* 1 à 1). La valeur de sa RM restera alors fixe par rapport à la devise par laquelle la couverture a été effectuée. S'il relie sa RM à une devise, avec une couverture complète, mais qu'il décide d'émettre par la suite de nouvelles unités, ayant une couverture incomplète, il dévaluera alors lentement sa RM (*peg* ou *crawling peg*, respectivement).

Enfin, si l'émission n'est pas reliée à une devise ou à un produit (tel que l'or, par exemple), la RM sera alors flottante par rapport à une devise en particulier. Notons que le taux de change d'une monnaie flottante varie dans le temps, tandis que le taux de change d'une monnaie couverte (que ce soit par *swap*, *peg* ou *crawling peg*) reste fixe ou varie seulement à l'intérieur d'une bande d'échange prédéterminée.

6.2.4 Infrastructures physiques

Nous avons vu dans la revue des systèmes de paiement électronique effectuée au début de cet ouvrage que plusieurs types de réseaux de communication peuvent être empruntés par différents environnements transactionnels, notamment des réseaux publics et des réseaux privés. Dans la perspective du développement des inforoutes en général et du commerce électronique en particulier, nous exprimons notre conviction que l'ordinateur, comme unité de calcul, de traitement et comme appareil ménager deviendra sous peu une unité tout aussi répandue et indispensable pour un appartement ou une maison, qu'un réfrigérateur ou une cuisinière. Alors, dans ce contexte, le réseau de communication s'estompera en arrière plan, tout comme le réseau électrique.

En effet, il n'est pas concevable aujourd'hui d'avoir une unité d'habitation sans un réseau électrique et, de la même manière, le réseau de communication deviendra tout aussi commun et irremplaçable. Les paiements électroniques, ainsi que les transferts numériques d'autres valeurs seront effectués, fort probablement, tout aussi facilement que n'importe quelle autre tâche courante.

Nous devons toutefois nous demander si ces transactions auront lieu sur des réseaux publics ou privés. À la limite, chaque système électronique de paiement pourra utiliser son propre réseau, public ou privé, comme support de transmission. Ainsi, les nouveaux systèmes de paiement ne devront pas absolument emprunter les réseaux publics; ceux-ci coexisteront avec des réseaux privés, du moins de façon théorique.

En pratique, toutefois, il est plus difficile de justifier économiquement la mise en place d'un réseau privé. Même si certains systèmes actuels basés strictement sur des réseaux privés ont déjà souvent un haut degré d'acceptation dans le monde entier – par exemple, les réseaux privés bancaires, ou ceux des compagnies de cartes de crédit

comme **VISA** ou **MasterCard** –, ces réseaux ne s'adressent pas aux petits détaillants virtuels ni aux consommateurs désireux de transiger à un prix minimal dans le confort de chez soi. Ils ne sont pas ouverts à la connexion de terminaux personnels privés. De plus, en ce qui concerne l'implantation des nouveaux systèmes de paiement électronique ayant comme support de communication des réseaux privés de communication, seul le coût d'installation de tels réseaux rend tout projet beaucoup moins compétitif à court et moyen terme. Leurs coûts d'entretien ne seront pas compensés, à notre avis, par les économies réalisées à l'aide de l'utilisation d'instruments transactionnels moins protégés, qui profitent de l'inaccessibilité et de l'opacité des réseaux privés. Donc, à long terme aussi, de tels systèmes seront encore moins compétitifs que ceux basés sur des supports ouverts.

L'alternative sera les réseaux de communication publics. Depuis plusieurs années déjà, ces réseaux constituent un support de plus en plus important pour les solutions généralement acceptées, qui ont un large appui dans leur industrie respective et qui relèvent d'un standard déjà implanté, testé et qui a fait ses preuves. Ceci n'implique aucunement que de nouvelles technologies ne feront pas leur apparition. Par exemple, la technologie du Web et du langage HTML – technologies qui datent seulement de quelques années – sont devenues aujourd'hui des standards dans la publication électronique, sur des supports ouverts, tels que le bien connu protocole TCP/IP, contrastant ainsi avec des systèmes qui ont échoué, tels que le système UBI ou Alex, le Minitel canadien, qui utilisait un protocole propre et fermé. Même le Minitel français enregistre aujourd'hui un déclin, après plusieurs années de décélération, au profit de l'Internet.

Ceci étant dit, nous devons remarquer que les réseaux publics de communication et les protocoles qui les régissent aujourd'hui ont leurs propres lacunes et imperfections. Notamment, la sécurité offerte par les protocoles utilisés aujourd'hui laisse à désirer. À cet égard, pour palier à ces limitations, nous croyons qu'une attention

particulière doit être portée au niveau de la conception [Abardi et Needham, 1996] et de la maintenance de tout système transportant des données ayant une valeur quelconque, et particulièrement pour les systèmes de paiement électronique. Ainsi, le nouveau protocole IP, le protocole IPv6, support de l'Internet de demain, apporte plusieurs remèdes aux lacunes que nous connaissons aujourd'hui.

Même les systèmes ayant un support de communication privé commencent à envisager une migration vers des solutions ouvertes et standardisées. Les banques et les compagnies de cartes de crédit étudient des moyens pour «ouvrir» leur environnement. Ainsi, les premières, offrent aujourd'hui la possibilité d'effectuer des opérations bancaires par téléphone ou même par Internet. Les secondes, se sont rassemblées pour concevoir et tester le protocole SET qui, une fois implanté à une échelle dépassant une masse critique, pourra remplacer leurs coûteux réseaux privés au profit des réseaux publics comme l'Internet.

Pour conclure sur ce point, nous croyons que les systèmes ayant un support de communication privé et ceux ayant un support de communication public pourront théoriquement coexister dans le «portefeuille virtuel» des consommateurs, tout comme plusieurs moyens différents de paiement coexistent aujourd'hui dans leur portefeuille réel. Toutefois, nous estimons que la probabilité d'avoir des solutions basées sur un support privé est radicalement plus réduite. La raison est simple: il est moins cher – et donc plus compétitif – de partager les coûts de communication avec tout le monde, en utilisant un réseau commun et public, ouvert à tous, même avec les risques afférents que cela comporte au niveau de la sécurité – risques qui peuvent être contournés à l'aide de systèmes tels que TRANZIX. Investir dans l'installation et la maintenance d'un coûteux réseau privé, fermé et disponible pour seulement une ou quelques applications spécialisées deviendra rapidement prohibitif.

6.2.5 L'épineuse question de l'anonymat

Une autre question très importante qui se pose – aujourd'hui détail technique, mais fort probablement un débat politique dans un avenir rapproché – concerne le niveau d'anonymat qui pourra être offert lors d'une transaction [Davies, 1997]. En effet, un niveau d'anonymat très élevé, implique évidemment une protection très efficace de la vie privée des consommateurs, mais permet en même temps l'épanouissement facile, rapide et incontrôlable des transactions illicites, car, dans les cas extrêmes, aucune trace ne peut être conservée.

Ceci nous amène au côté politique du problème de l'anonymat. Ainsi, il est bien connu que de nombreux consommateurs, partout à travers le monde, auront tendance à limiter ou éliminer leurs obligations sous forme de taxes et impôts envers leurs gouvernements. Ayant la possibilité théorique de transférer leurs économies de façon anonyme vers des paradis fiscaux, les consommateurs pourraient priver ainsi les autorités de leur pouvoir de taxation ce qui, à moyen et long terme, pourrait mener à l'anarchie. Interdire l'argent virtuel n'est pas une solution: non seulement il s'agirait d'une décision rétrograde, mais il s'agirait aussi d'une décision impraticable. En effet, un message encrypté contenant des billets numériques peut facilement être dissimulé à l'intérieur d'un autre fichier binaire contenant, par exemple, une image quelconque.

Regardons un autre aspect de cette question. Si aujourd'hui les autorités essayent de rendre de plus en plus difficile le blanchiment d'argent, les systèmes anonymes de paiement auraient un effet inverse, rendant la tâche non seulement facile, mais aussi rapide et peu coûteuse. Que faire alors ? Promulguer des lois interdisant les transactions numériques ? Interdire toutes les communications, démonter les réseaux terrestres et les satellites de communication ? Comme toute loi interdisant certains droits ou privilèges des consommateurs n'aurait effet que dans le pays où elle a été adoptée, la

portée mondiale du réseau Internet rend une telle mesure inapplicable[4] au niveau international. Comme la difficulté d'imposer des lois ayant une portée internationale est quasi insurmontable, le résultat prendra la forme du plus petit dénominateur commun: les lois les plus permissives et tolérantes auront prépondérance, car tout serveur peut déménager virtuellement en peu de temps n'importe où sur la planète.

À cet égard, nous estimons qu'une grande importance sera rattachée aux réactions des gouvernements, réactions qui pourront fixer les grandes directions de développement futur. Plusieurs pays ont déjà établi des politiques en matière de commerce électronique, comme nous allons le voir dans les pages suivantes. À notre avis, l'état ne devra pas réagir brutalement contre des technologies naissantes; une telle réaction découragera le développement naturel et encouragera les solutions illicites. Par contre, si rien n'est fait, des problèmes tels que ceux décrits plus haut apparaîtront avec une très grande probabilité. Le rôle et l'influence de l'état seront donc déterminantes pour éviter le chaos [Kelley, 1997].

Un système monétaire ne peut survivre sans un minimum de confiance mutuelle entre les différents intervenants. Ainsi, la confiance générale dans un système est déterminée par la confiance que les clients ont dans les banques, comme détenteurs de leurs économies, la confiance que les vendeurs, à leur tour, doivent avoir dans le protocole qui leur assure la réception des fonds une fois la marchandise livrée, la confiance que tous ces intervenants ont dans les émetteurs et dans sa RM émise, la confiance dans les moyens de résolution de conflits, de disputes et ainsi de suite. Même un système totalement opaque, assurant un niveau complet et inconditionnel d'anonymat requiert un minimum de confiance dans l'émetteur, dans sa capacité de gérer la masse

[4] Regardons un exemple: lors des récentes élections législatives en France, une loi interdisait la publication de tout sondage ou résultat partiel pendant un certain intervalle de temps avant et pendant la tenue des élections. Or ces sondages, et même des résultats partiels, étaient disponibles, pendant l'intervalle de temps concerné, sur des serveurs Web suisses ou belges.

monétaire réelle et virtuelle et dans la qualité de sa RM; un niveau minimal de confiance est aussi nécessaire quant à la crédibilité de l'état – comme législateur garant des lois et règlements. Nous allons considérer comme axiomatique cette quantité minimale mais indispensable de confiance.

Plusieurs solutions préventives peuvent être prises bien en avance par les institutions et organisations concernées. Ainsi, par exemple, l'état pourrait établir un cadre juridique qui encourage le développement des solutions raisonnables et crédibles; l'état pourrait établir une autorité centrale pouvant émettre des signatures électroniques en format standardisé, reconnaissables par tous les intervenants; une banque centrale pourrait émettre des billets numériques ayant cours légal et une valeur égale aux devises réelles. Enfin, l'état pourrait montrer une préférence pour un système ou un ensemble de systèmes transactionnels offrant des solutions acceptables pour tous les intervenants, entraînant ainsi une majorité de consommateurs à suivre son exemple.

Aujourd'hui, dans chaque système transactionnel ou informationnel, des solutions optimales – à plusieurs niveaux du design – doivent être recherchées et implantées; ainsi, dans le système TRANZIX, au niveau de l'anonymat offert lors du déroulement d'une transaction – et dans le système en général – nous proposons, comme nous l'avons déjà mentionné, des solutions de compromis. En se basant sur la crédibilité des émetteurs et de l'état, le système TRANZIX vise à offrir un juste milieu entre l'anonymat parfait et un manque total de confidentialité.

Deux aspects contribuent à cette solution de compromis: les informations de trace, qui permettent de retracer le parcours d'une transaction en général et d'un billet en particulier, et les moyens cryptographiques qui permettent d'offrir une réelle confidentialité aux usagers, en dissimulant ces traces, de façon à les rendre invisibles pour tout accès non autorisé. Tout d'abord, le système doit disposer d'une quantité d'information suffisante pour assurer une trace claire et distincte de toute transaction.

Cette trace se trouve, de façon redondante, tant dans les fichiers de trace du client que dans celles du vendeur – car les deux parties voudrons avoir la trace de leurs transactions. De plus, tous les dépôts, retraits ou échanges de coupures sont aussi notés dans les fichiers de trace de la banque.

Concrètement, en plus d'une signature numérique unique, nous avons montré comment un ID-biométrique est assigné à chaque usager, permettant de l'identifier correctement. Les émetteurs entrent aussi en jeu à ce niveau: ils doivent s'assurer de la collecte complète de toutes les informations qui leurs sont nécessaires. Tous ces aspects sont conçus pour suivre la trace des transactions et l'application des lois et des règlements en vigueur à travers le système transactionnel. En ce qui concerne la confidentialité, nous avons présenté dans le Chapitre 4 les moyens cryptographiques à l'aide desquels nous pouvons assurer les usagers que seulement les personnes concernées, peuvent accéder aux informations confidentielles.

De plus, des limites sont imposées sur la quantité de valeur véhiculée dans des transferts non contrôlés – comme c'est le cas dans le cadre des autres environnements économiques. Ainsi, TRANZIX offre à l'émetteur la possibilité d'établir une limite sur le montant des transactions qui peuvent être effectuées – couramment 1000 dollars dans notre prototype, tel que spécifié par les lois canadiennes. Le transfert d'une importante quantité d'argent – un million de dollars, par exemple – impliquerait alors un nombre important de transactions et de connexions – mille, pour le cas de l'exemple précédent. Ceci est facilement réalisable, de façon automatique par le logiciel; mais la trace laissée par un aussi grand nombre de transactions dans un court intervalle de temps sera suffisamment claire pour être détectée par l'émetteur et donc par les autorités.

De cette façon, l'état, les émetteurs et les consommateurs en général sont protégés contre les utilisations illicites du système, en assurant, d'une part, une trace

suffisamment détaillée pour faire le suivi des transactions récentes, et d'autre part, suffisamment difficile à acquérir légalement. Les usagers, notamment, sont protégés contre le suivi de leurs transactions ou autre manque de confidentialité par l'encryptage de leurs messages transactionnels et par la dissimulation des informations biométriques se trouvant à l'intérieur des paquets qui circulent sur le réseau[5]. Le système pourra ainsi fonctionner sur la base des arguments mathématiques et techniques facilement quantifiables, plutôt que d'autres – tels que la popularité momentanée générée par des campagnes publicitaires.

6.3 Initiatives gouvernementales

Les gouvernements de nombreux pays ont déjà élaboré des politiques concernant les inforoutes en consacrant une place importante au commerce électronique. La question du paiement électronique sur Internet n'a pas été souvent abordée comme enjeu, étant plutôt reléguée au niveau d'une mesure technique qui devra être réglée par des spécialistes. Ces politiques de commerce électronique évoquent les aspects à régler afin de favoriser les transactions numériques entre entreprises et avec les consommateurs.

Dans la plupart des cas, il s'agit de critères permettant de respecter la confidentialité des transactions et des intervenants, d'authentifier ces intervenants, d'assurer l'intégrité des informations transmises ou d'offrir des mécanismes garantissant la non-répudiation des transactions afin d'encourager les entreprises à offrir leurs

[5] Évidemment, tel que discuté dans le Chapitre 4, la collusion entre différentes entités pourrait – comme dans n'importe quel autre environnement transactionnel – déjouer, dans certains cas, les protections qui sont généralement assurées.

services sur l'Internet [Bégin et Tellier, 1999]. D'autres aspects souvent mentionnés concernent les technologies permettant d'assurer la sécurité – notamment les technologies cryptographiques – des communications, le commerce inter-régional et international, la taxation, etc.

Au Québec, la «Politique québécoise des autoroutes de l'information», rendue publique en avril 1998, réserve une place importante au commerce électronique et à l'Internet en général. Ainsi, les protocoles et les standards de l'Internet deviennent la norme gouvernementale privilégiée pour les communications numériques. Le commerce électronique est identifié comme un secteur à part entière dans lequel le gouvernement s'engage à investir et à inciter le secteur privé à faire de même.

Au niveau canadien, «La politique cadre en matière de cryptographie aux fins du commerce électronique: Pour une économie et une société de l'information au Canada» [Référence électronique PCMC] a été déposée en 1998, suite à une consultation publique. Parmi les facteurs dont le gouvernement fédéral devra tenir compte dans sa politique en matière de cryptographie nous retrouvons le rôle essentiel des réseaux ouverts, tels que l'Internet, dans son déploiement à l'échelle nationale, ainsi que le rôle indispensable de la cryptographie pour assurer un haut niveau de sécurité aux transmissions de données.

Les États-Unis ont aussi formulé plusieurs politiques et plans d'actions. Le développement rapide des outils de paiement numérique et du commerce électronique en général incite le gouvernement américain à exclure tout dirigisme et toute position rigide dans l'imposition d'un règlement ou dans le choix d'une ou de plusieurs solutions. Si le gouvernement américain préfère à court terme les tests et les projets pilotes, à long terme, il reconnaît que l'autorégulation de l'industrie ne pourra régler tous les problèmes actuels et futurs [Référence électronique FGEC].

Au niveau de la taxation, les États-Unis et le Japon ont publié un communiqué commun en faveur d'une liberté fiscale du commerce sur Internet, exprimant leur volonté de faire de cette grande confédération de réseaux publics une zone sans taxes. Alors que l'Union Européenne a accepté les principes de cette proposition, la plupart des pays de l'OCDE sont inquiets de l'explosion potentielle des activités bancaires en-ligne. Pour répondre à ces craintes, les États-Unis ainsi que le Japon ont promis de travailler avec les experts de l'OCDE pour mettre en place des systèmes permettant d'éviter les éventuelles fraudes fiscales.

6.4 Conclusion

En quelques années seulement, l'Internet a évolué rapidement, en partant d'un réseau de communication très spécialisé, réservé aux scientifiques, pour devenir un «marché virtuel» viable et prospère. Des bases de données centrées sur Internet permettent aux commerces d'anticiper les besoins de leurs clients et de personnaliser ainsi leurs produits et services à un niveau sans précédent. En même temps, une nouvelle compétition intersectorielle se développe pendant que les barrières entre les industries tombent. L'Internet a aussi aidé autant les consommateurs que les institutions commerciales à transcender les frontières géographiques et a accentué le mouvement vers la libéralisation du commerce et la déréglementation des marchés; ainsi, le monde est devenu tant client que compétiteur.

La numérisation a conduit à des produits et des services complètement nouveaux; les publications électroniques, les services financiers en-ligne, les achats et ventes aux enchères numériques sont là quelques exemples des tendances qui émergent. Les relations interentreprises sont transformées: les fournisseurs deviennent des

partenaires et partagent ensemble les profits et les risques. Il est utile de remarquer le fait que l'analyse de ces nouveaux aspects du commerce électronique ouvre des perspectives très intéressantes pour des études économiques à plusieurs niveaux, tels que les moyens de gérer la création et la croissance de la masse monétaire virtuelle, les moyens de localiser les parties pertinentes à la solution d'un problème de fraude lorsque la base de données de la banque est très vaste, le dépistage des transactions illicites en regardant certaines tendances ou motifs (*patterns*) transactionnels, ainsi que les habitudes des fraudeurs, etc. De telles études seront extrêmement utiles – et même nécessaires – pour clarifier davantage plusieurs aspects mentionnés précédemment et pour répondre à certaines des questions soulevées dans ce chapitre, permettant ainsi à tous les intervenants d'effectuer les meilleurs choix en matière de systèmes transactionnels, de manière informée et en toute connaissance de cause.

Nous venons d'effectuer une très brève incursion dans un domaine assez complexe qui combine l'informatique appliquée avec la politique économique. Des études complètes d'impact seront nécessaires pour clarifier l'avenir des échanges commerciaux électroniques, qui ne tarderont à prendre un pourcentage de plus en plus important du marché global d'échanges commerciaux. En étudiant le passé et en regardant vers l'avenir, un constat peut être fait sans hésitation: une nouvelle forme de monnaie s'en vient et sera accompagnée fort probablement d'une nouvelle méthode de transport de valeurs et de stockage pour une utilisation future. À court terme de tels systèmes transactionnels rempliront les besoins d'une niche du marché; mais à moyen et à long terme, nous avons la conviction qu'ils occuperont une proportion substantielle parmi tous les autres instruments permettant des échanges de valeurs. Le commerce électronique, qui a déjà un taux de croissance élevé, prendra ainsi une place de choix, devant les autres formes d'échange économique.

CHAPITRE 7

CONCLUSIONS GÉNÉRALES

Nous voici à la fin de cet ouvrage, dans lequel nous avons voulu entreprendre un imposant travail de recherche, d'évaluation, de création et d'analyse. Concrètement, en se basant sur une recherche bibliographique détaillée, nous avons évalué l'état de l'art du domaine des systèmes électroniques de paiement afin de faire ressortir les besoins d'un nouveau système transactionnel. Nous avons introduit de nouveaux concepts et de nouvelles notions sur lesquelles nous nous sommes basés pour créer ce nouveau système. Enfin, nous avons analysé plusieurs caractéristiques du nouveau système à l'aide d'un prototype expérimental et nous avons discuté de certains aspects techniques et socio-économiques associés à l'implantation d'un tel système. De cette manière, nous avons accompli notre mandat en réalisant tous les objectifs que nous nous sommes fixés au début de notre travail et que nous avons mentionnés au Chapitre 3.

Nous avons débuté cet ouvrage en effectuant une mise en contexte de notre travail et nous avons présenté brièvement le contenu de cette thèse. Dans le deuxième chapitre, après avoir introduit une nouvelle taxonomie et plusieurs critères d'analyse, nous avons compilé un tableau d'évaluation détaillé, comprenant un grand nombre de

systèmes électroniques de paiement sur Internet. La plupart de ces systèmes répliquent et transposent des systèmes monétaires du «monde réel» dans le cyberespace, d'autres offrent des moyens innovateurs pour transiger. Il est évident qu'aucun système ne pourra répondre à tous les besoins de tous les intervenants; la plupart des systèmes, protocoles et méthodes de paiement électronique comportent des avantages et des désavantages.

Au Chapitre 3, nous avons fait ressortir les besoins d'un nouveau système de transfert numérique de valeurs. Nous avons introduit de nouveaux concepts, généralisant les notions présentes et nous avons utilisé ces nouveaux concepts pour établir les bases d'un nouveau système transactionnel, que nous avons appelé TRANZIX.

Le quatrième chapitre nous a permis de présenter en détail les caractéristiques générales du système TRANZIX en présentant ses spécifications fonctionnelles, notamment le flux informationnel entre les entités transactionnelles. Nous avons proposé, par la suite, le design préliminaire du nouveau système transactionnel, basé sur les contraintes et les besoins que nous avions soulignés, en tenant compte des utilisations des différents intervenants impliqués dans une transaction. Le nouveau système électronique de transfert numérique de valeurs permet, en plus des transferts de fonds électroniques, l'échange de toute valeur qui peut être représentée directement ou indirectement sous format numérique. Nous avons défini les différents centres de traitements et leurs tâches afférentes, nous avons présenté le diagramme hiérarchique et la structure des données du système et nous avons décrit ses interfaces. Après avoir exposé les principaux éléments qui nécessitent une protection particulière, nous avons décrit les détails du design ainsi que les instruments de protection que nous employons. Nous avons expliqué comment la sécurité du nouveau système, vu globalement, pourrait être assurée à l'aide de moyens cryptographiques et biométriques.

TRANZIX offre un très haut niveau de sécurité, protégeant les données contenues dans les enveloppes virtuelles à l'aide des technologies cryptographiques. Ainsi, le contrôle d'accès au système et aux données qui y circulent est assuré par un encryptage fort; l'encryptage assure aussi la confidentialité des données transportées tandis que l'intégrité de ces données ainsi que l'authentification des intervenants sont assurées à l'aide de signatures numériques. L'authentification est renforcée à l'aide des moyens biométriques qui nous permettent aussi d'assurer la non-répudiation des transactions.

À l'aide d'un prototype squelettique expérimental implanté sous forme logicielle, que nous avons présenté au Chapitre 5, nous avons simulé le comportement du système global en fonction des principales contraintes de design mentionnées dans les chapitres précédents. Plusieurs applications ont été présentées, incluant l'accès contrôlé à des ressources physiques et virtuelles, ainsi que l'échange personnalisé de documents sécurisés et les transferts mixtes de valeurs.

Nous avons regardé les différents aspects portant sur le temps de génération des clés cryptographiques et sur le temps de transaction. Nous avons ainsi démontré la nécessité d'arriver à un compromis entre le niveau de sécurité désiré et la vitesse de calcul disponible, en tenant compte des applications pour lesquelles le système sera utilisé et du contexte dans lequel les transactions auront lieu. Des moyens d'optimisation ont aussi été proposés.

Enfin, nous avons discuté au Chapitre 6 des principaux impacts socio-économiques que les systèmes transactionnels, tels que TRANZIX, pourraient avoir sur les différents intervenants et sur le commerce électronique en général. Nous avons esquissé différents aspects concernant les types d'émission, de couverture et d'infrastructure physique envisageable et nous avons discuté de l'anonymat et des impacts qu'il pourrait avoir. Nous avons avancé que le succès de tout nouveau système

transactionnel sera déterminé par les consommateurs qui évalueront une combinaison de facteurs, incluant la commodité et la facilité d'utilisation, la rapidité, la sécurité, les coûts afférents, ainsi que le nombre et la qualité des vendeurs disposés à offrir leurs biens et services contre cette nouvelle forme de représentation monétaire.

7.1 Contributions originales

Cette thèse nous a permis d'apporter des contributions originales au développement d'une solution viable, sécuritaire et performante au problème de transfert numérique de documents électroniques et de fonds virtuels. Tout d'abord, nous avons introduit une nouvelle taxonomie, assortie d'une liste de critères d'analyse qui nous a permis de réaliser une première revue quasi exhaustive des systèmes électroniques de paiement sur Internet. Cette étude s'est avérée très efficace dans le cheminement de notre travail et, nous l'espérons, elle sera aussi utile pour quiconque envisage d'installer et d'exploiter de tels systèmes à partir d'une plate-forme de commerce électronique.

Dans un deuxième temps, nous avons introduit de nouveaux concepts, généralisant la notion de paiement comme valeur transigée et comme opération transactionnelle. Nous avons ainsi crée un instrument unique de transport, de transfert et d'échange de valeurs numériques, permettant de transiger tout objet virtuel ou objet réel pouvant être représenté numériquement. Nous avons aussi introduit la notion d'enveloppe virtuelle que nous avons employée pour introduire un nouveau protocole, le PTEV, sur lequel un nouveau système transactionnel, TRANZIX, est basé.

TRANZIX permet non seulement de généraliser les opérations transactionnelles, mais aussi de généraliser la notion de valeur. De cette manière, TRANZIX peut transiger tout objet virtuel, de l'argent numérique aux documents électroniques, en passant par les «cyberjetons» et les certificats numériques. Ainsi, nous avons réussi à introduire un nouveau type de transaction numérique, les transactions mixtes, permettant les échanges concurrents de différents types de valeurs.

Le système TRANZIX est le premier à utiliser une approche bimodale donnant aux usagers le choix du mode de communication en-ligne ou hors-ligne ainsi que celui du support physique pour cette communication. Un autre élément original réside au niveau de la sécurité assurée à l'aide des technologies de protection utilisant des moyens biométriques d'identification. Ces moyens innovateurs permettent non seulement de personnaliser les signatures numériques des utilisateurs et donc les enveloppes virtuelles servant au transport des données, mais ils permettent aussi d'être interchangés en fonction du niveau de sécurité requis par une application donnée.

En ce qui concerne l'aspect monétique, notre système a démontré une façon ingénieuse de combiner les avantages de certains systèmes existants – voire l'utilisation des billets virtuels prépayés, la communication hors-ligne et les micropaiements; en même temps il permet d'éliminer certains désavantages et limites trouvés dans d'autres systèmes – tels que ceux employant les cartes de crédit –, tout en apportant des solutions innovatrices à plusieurs niveaux du design. Ainsi, la manière par laquelle nous avons proposé l'utilisation de la communication hors-ligne rend économiquement viable le concept de micropaiements. TRANZIX innove aussi en permettant l'émission privée de certificats numériques – et même de monnaie privée. Les moyens de vérification permettant une approche décentralisée et le compromis réalisé au niveau de l'anonymat offrent des solutions uniques qui pourraient s'avérer très utiles lors d'un éventuel déploiement commercial à large échelle.

7.2 Directions possibles des futurs développements

Le travail que nous avons entrepris nous a permis d'introduire un nouveau système transactionnel permettant le transfert généralisé de valeurs, sans restrictions au niveau de ce qu'elles représentent. Nous allons regarder brièvement dans cette section comment le système pourrait être amélioré, comment le protocole expérimental que nous avons réalisé pourrait être développé pour arriver à un produit commercial et quelles seront les bénéfices potentiels qui pourront être envisagés.

Tel que spécifié dans le Chapitre 5, le logiciel que nous avons conçu est un prototype squelettique expérimental servant à démontrer la faisabilité des concepts introduits et à évaluer certaines caractéristiques. Pour un éventuel déploiement à large échelle, suivant le modèle conceptuel complet, un ensemble de logiciels ayant une qualité commerciale, avec le support technique et documentaire nécessaire, devrait être envisagé. La documentation devra ainsi s'adresser à tous les niveaux de connaissances et d'expérience des systèmes transactionnels des usagers potentiels et elle devra être rédigée en plusieurs langues. L'interface, qui permettra l'interaction humaine sera graphique, ergonomique et explicite, en réduisant au minimum les besoins d'apprentissage de commandes complexes.

En guise de tout premier pas vers une éventuelle optimisation, nous avons ajouté les rudiments d'un support pour des interfaces plurilingues, utilisant une approche non-centralisée. Concrètement, les messages textuels représentant les interactions du système avec les usagers ne sont plus codés directement dans le logiciel; ces messages sont remplacés par des étiquettes qui pointent vers des messages se trouvant dans des fichiers externes. De cette manière, en respectant l'ordre et la

numérotation préétablie des étiquettes, ces fichiers pourront contenir les traductions en d'autres langues des messages textuels, permettant ainsi l'internationalisation du système. En même temps, étant donné le fait que ces fichiers sont externes au logiciel, ils peuvent être réalisés de façon distribuée, dans nécessiter une nouvelle compilation des logiciels formant le système.

Le système pourra ainsi être implanté de façon modulaire, permettant d'intégrer des modules de langues différentes; il permettra de plus à l'usager de transiger dans la devise de son choix et d'ajouter d'autres modules externes (*plug-ins*), par exemple, des outils pour l'échange de devises, des instruments financiers d'investissements, etc. En fonction des politiques gouvernementales des différents pays concernant l'utilisation et l'exportation des technologies cryptographiques [Rivest, 1998], une idée intéressante d'optimisation serait de donner à l'émetteur la possibilité de choisir la méthode et les algorithmes d'encryptage et de signature numérique, ainsi que l'intervalle de puissance (proportionnelle à la longueur en bits) des clés à utiliser. Les utilisateurs auraient ainsi la possibilité non seulement d'interchanger les outils cryptographiques utilisés, mais aussi d'employer des clés distinctes, de longueurs différentes, en fonction de l'importance qu'ils accorderont à une transaction donnée.

7.3 Perspectives d'avenir

Les nouvelles technologies, permettant le transfert facile, rapide et sécuritaire de valeurs sur des réseaux publics de communication, auront un impact social non-négligeable, surtout au niveau des habitudes transactionnelles des consommateurs. À notre avis, il est probable que l'apparition d'un nouveau type de système transactionnel n'impliquera pas nécessairement la disparition d'un autre, tout

comme les différents moyens de paiement d'aujourd'hui: les cartes de débit n'ont pas amené l'élimination des cartes de crédit, tout comme l'apparition de **MasterCard** n'a pas signifié la disparition de **VISA**. Nous estimons qu'une variété tout aussi grande d'instruments transactionnels survivra aussi dans le monde du commerce électronique.

En ce qui concerne le système TRANZIX, il pourrait être, à notre avis, un nouveau joueur sur la scène du commerce électronique. En partant de l'idée de combler le vide laissé par les manques et les défauts détectés dans les systèmes existants et en s'appuyant sur plusieurs de leurs points forts, tout en apportant plusieurs solutions innovatrices, TRANZIX pourra se démarquer facilement. Il surpasse la plupart des solutions qui se trouvent dans la catégorie débit/crédit par sa flexibilité et sa sécurité. Il tire profit de ses capacités à effectuer des transactions hors-ligne, ainsi que des micropaiements, égalant ou même surpassant ainsi la plupart des systèmes utilisant des pièces numériques.

En même temps, il peut concurrencer de façon très compétitive les systèmes basés sur l'utilisation des cartes de crédit en étant un système direct et symétrique, qui offre aux consommateurs la possibilité d'embarquer facilement, indépendamment de leur dossier de crédit. Il offre des transferts de fonds à moindre coût de traitement et une vitesse d'acquittement – du moins théorique – plus élevée que celle des centres de cartes de crédit. De plus, TRANZIX est le seul système à ce jour à offrir une solution générale, capable de transférer toute autre valeur numérique, en plus de l'argent. Tout aussi intéressante est la grande portabilité du logiciel, portabilité que le langage Java lui confère automatiquement.

D'autres aspects reliés aux systèmes transactionnels font aujourd'hui l'objet d'autres études dans le monde académique, dans différentes disciplines reliées au commerce électronique. Ainsi, par exemple, au niveau de la sécurisation, des nouveaux algorithmes d'encryptage sont proposés, étudiés ou réexaminés, tels que ceux

employant les logarithmes discrets [ElGamal, 1985] ou les courbes elliptiques; d'autres protocoles cryptographiques viennent d'être proposés, tels que ceux qui emploient les signatures aveugles de groupe ou l'anonymat révocable. De telles méthodes, combinées à des méthodes d'intégration des technologies basées sur les cartes intelligentes, ainsi que des approches optimisées pour le transfert généralisé de fonds et de valeurs, constituent seulement quelques-unes unes des avenues les plus prometteuses de développement futur.

Nous estimons qu'aucune solution unique n'émergera toute seule, une multitude d'outils électroniques pour effectuer des transactions prévaudront, chaque solution remplissant un ou plusieurs besoins spécifiques et particuliers, tout comme dans le monde réel aujourd'hui: un portefeuille réel contient plusieurs cartes de crédit, quelques cartes de débit, quelques billets de banque et possiblement des chèques ou des pièces de monnaie. À notre avis, tout comme dans le monde réel actuel où plusieurs moyens de paiement coexistent dans le portefeuille réel des consommateurs, plusieurs systèmes transactionnels et moyens de paiement numérique seront présents dans le portefeuille virtuel du consommateur de demain. Quelle solution transactionnelle numérique pourrait faire partie des portefeuilles virtuels de demain sera sans doute décidé par les consommateurs, seuls à savoir quels systèmes pourrons servir mieux leurs besoins et intérêts particuliers dans l'économie virtuelle de l'avenir.

BIBLIOGRAPHIE

ABARDI, M. and NEEDHAM, R. (1996): «Prudent Engineering Practice for Cryptographic Protocols», *IEEE Transactions on Software Engineering*, Vol. 22, No. 1, January 1996.

AMMAR, M., YOSHIDA, Y. and FUKUMURA, T. (1990): «Structural Descritption and Classification of Signature Images», *Pattern Recognition*, Vol. 23, No. 7, pp. 697-710, Pergamon Press, 1990.

ANDERSON, H. (1997): «Money and the Internet: a Strange New Relationship», *IEEE Computer*, January 1997.

ASOKAN, N., JANSON, P. A., STEINER, M. and WAIDNER, M. (1997): «The State of the Art in Electronic Payment Systems», *IEEE Computer*, September 1997.

ATKINSON, R. J. (1997): «Toward a More Secure Internet», *IEEE Computer*, January 1997.

BÉGIN, F. et TELLIER, S. (1999): «Paiement électronique sur Internet: Politiques et réglementation», *Direction informatique*, vol. 12, no. 5, mai 1999.

BELOTTI, V. (1997): «Design for Privacy in Multimedia Computing and Communications Environments» in «*Technology and Privacy: The New Landscape*», edited by Philip E. AGRE and Marc ROTENBERG, The MIT Press, 1997.

BRANDS, S. (1994a): «An Efficient Off-line Electronic Cash System Based on the Representation Problem», *CWI Publications*, Amsterdam, 1994.

BRANDS, S. (1994b): «Off-line Cash Transfer by Smart Cards», *CWI Publications*, Amsterdam, 1994.

BRANDS, S. (1995a): «Electronic Cash on the Internet», *Proceedings of the Internet Society 1995 Symposium on the Network and Distributed System Security*, San Diego, California, 1995.

BRANDS, S. (1995b): «Off-line Electronic Cash Based on Secret-Key Certificates», *Proceedings of the Second International Symposium of Latin American Theoretical informatics*. Valparaiso, Chili, April 1995.

BURKERT, H. (1997): «Privacy-Enhancing Technologies: Typology, Critique, Vision» in «*Technology and Privacy: The New Landscape*», edited by Philip E. AGRE and Marc ROTENBERG, The MIT Press, 1997.

BÜRK, H. and PFITZMANN, A. (1989): «Digital Payment Systems Enabling Security and Unobservability», *Computers & Security*, August 1989.

CHAUM, D. (1981): «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms», *Communications of the ACM*, Vol. 24, No. 2, February 1981.

CHAUM, D. (1983): «Blind Signatures for Untraceable Payments» in D. CHAUM, R. L. RIVEST and A. SHERMAN, editors, *Advances in Crypotolgy – Proc. CRYPTO '82*, Plenum Press, 1983, pp. 199-203.

CHAUM, D. (1989): «Privacy Protected Payments Unconditional Payer and/or Payee Untraceability», *SmartCard 2000*, North-Holland, 1989.

CHAUM, D., FIAT, A. and NAOR, M. (1990): «Untraceable Electronic Cash» in S. GOLDWASSER, editor, «*Advances in Cryptology – CRYPTO '88*», v. 403 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 319-327.

CHAUM, D. (1991): «Online Cash Checks», *CWI Publications Amsterdam*, 1991.

CHAUM, D. (1992): «Achieving Electronic Privacy», *Scientific American*, August 1992.

CHAUM, D. and BRANDS, S. (1997): «'Minting' Electronic Cash», *IEEE Spectrum*, February 1997.

COX, B., TYGAR, J. D. and SIRBU, M. (1995): «NetBill Security and Transaction Protocol», *Proceedings of the First Usenix Electronic Commerce Workshop*, Usenix, Berkeley, California, 1995.

DAVIES, S. G. (1997): «Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity» in «*Technology and Privacy: The New Landscape*», edited by P. E. AGRE and M. ROTENBERG, The MIT Press, 1997.

DENNING, D. E. R. (1982): «*Cryptography and Data Security*», Addison-Wesley, 1982.

DJEZIRI, S., NOUBOUD, F. and PLAMONDON, R. (1997): «Extraction of Items from Checks», in *Proceedings of the 4th International Conference on Document Analysis and Recognition (ICDAR '97)*, Ulm, Germany, August 1997.

ELGAMAL, T. (1985): «A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms», *IEEE Transactions on Information Theory*, 31, 1985, pp. 469-472.

FANCHER, C. (1997): «In Your Pocket: Smartcards», *IEEE Computer*, January 1997.

FDA (Food and Drug Administration), Department of Health and Human Services (1997): «CFR Part 11 – Electronic Records; Electronic Signatures; Final Rule; Electronic Submissions; Establishment of Public Docket; Notice», *Federal Register*, Part II, Vol. 62, No. 54, March 20, 1997, p. 13440.

FERGUSON, N. (1993): «Single Term Off-line Coins», *Centrum voor Wiskunde en Informatica Report*, 1993.

FLOHR, U. (1996): «Electric Money», *BYTE*, June 1996.

FORD, W. (1998): «Digital Certificates», *Scientific American*, Vol. 279, No. 4, October 1998, p. 108.

GALLANT, J. (1995): «Smart Cards – Trained for Security», *EDN*, November 1995.

HAMILTON, S. (1997): «E-Commerce for the 21st Century», *IEEE Computer*, May 1997.

HEIN, T. R., NEMETH, E., SEEBASS S. and SNYDER, G. (1995): «*Unix System Administration Handbook*», Prentice Hall, 1995.

HEINTZE, N. and TYGAR, J. D. (1996): «A Model for Secure Protocols and Their Compositions», *IEEE Transactions on Software Engineering*, Vol. 22, No. 1, January 1996.

HONG T., WU, S. and SRIHARI, S. N. (1996): «Evaluating Japanese Document Recognition in the Internet/Intranet Environment», in *Proceedings of Workshop on Document Analysis Systems*, Malvern, Pennsylvania, Oct. 14-16, 1996.

KAMBIL, A. (1997): «Doing Business in the Wired World», *IEEE Computer*, May 1997.

KAUFMAN, C., PERLMAN, R. and SPECINER, M. (1995): «*Network Security – Public Communication in a Public World*», Prentice Hall, 1995.

KELLEY, E. W. Jr. (1997): «The Future of Electronic Money: a Regulator's Perspective», *IEEE Spectrum*, February 1997.

LECLERC, F. and PLAMONDON, R. (1994): «Automatic Signature Verification: 1989-1993», *International Journal of Pattern Recognition and Artificial Intelligence, Special issue on Signature Verification*, vol. 8, no 3, 1994, pp. 643-660.

LEE, S. and PAN, J. C. (1992): «Offline Tracing and Representation of Signatures», *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 22, No. 4, July/August 1992.

LÉPINAY, S. et AUDET, M. (1999): «Un nouveau consommateur est né», Réseau CEFRIO, Vol. 1, No. 1, Janvier 1999, pp. 3-8.

LOW, S., MAXEMENCHUCK, F. N. and SANJOY, P. (1994): «Anonymous Credit Cards», *Proceedings of the 2nd ACM Conference on Computer and Communication Security*, Fairfax, Virginia, 1994.

MALLAT, S. G. (1986): «A Theory for Multiresolution Signal Decomposition: The Wavelet Representation», *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 11, No. 7, July 1986.

MANASSE, M. S., GLASSMAN, S., ABADI, M., GAUTHIER, P. and SOBALVARRO, P. (1995): «The MilliCent Protocol for Inexpensive Electronic Commerce», *Proceedings of the First USENIX Workshop on Electronic Commerce*, California, 1995.

MAAT, M. (1997): «The Economics of E-cash», *IEEE Computer*, January 1997.

MARTIN, J. (1994): «*Design of Real-Time Computer Systems*», Prentice-Hall, 1994.

McCHESNEY, M. C. (1997): «Banking in Cyberspace: an investment in itself», *IEEE Computer*, January 1997.

MEYER, C. H. and MATYAS, S. M. (1982): «*Cryptography: A New Dimension in Computer Data Security*», John Wiley & Sons, 1982.

NETBANK (1995): «*Introduction to NetBank*», Software Agents, 1995.

OPPLIGER, R. (1996): «*Authentication Systems for Secure Networks*», Artech House, 1996.

OPPLIGER, R. (1997): «Internet Security: Firewalls and Beyond», *Communications of the ACM*, Vol. 40, No.5, May 1997.

PHILLIPS, D. J. (1997): «Cryptography, Secrets, and the Structuring of Trust» in «*Technology and Privacy: The New Landscape*», edited by Philip E. AGRE and Marc ROTENBERG, The MIT Press, 1997.

PLAMONDON, R. and LORETTE, G. (1989): «Automatic Signature Verification and Writer Identification: The State of the Art», *Pattern Recognition*, vol. 22, no 2, 1989, pp. 107-131.

PLAMONDON, R., LORETTE, G. and SABOURIN, R. (1990): «Automatic Processing of Signature Images: Static Techniques and Methods», in R. PLAMONDON, C. G. LEEDHAM, editors, *Computer Processing of Handwriting (Book of selected papers from 4th IGS Conference on Pattern Recognition)*, World Scientific Publishing, 1990, pp. 49-63.

PLAMONDON, R. (1994): «The Design of an On-Line Signature Verification System: From Theory to Practice», *International Journal of Pattern Recognition and Artificial Intelligence, Special Issue on Signature Verification*, vol. 8, no 3, 1994, pp. 795-811.

PORAT, M. (1977): «*The Information Economy*», US. Office of Telecommunications, 1977.

PRATT, W. K. (1978): «*Digital Image Processing*», Wiley Interscience, 1978.

RARAN, N. (1995): «Birth of an Electronic Nation», *BYTE*, July 1995.

RIVEST, R. L., SHAMIR, A. and ADLEMAN, L. M. (1978): «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems», *Communications of the ACM*, Vol. 21, No. 2, Feb. 1978.

RIVEST, R. L. (1998): «The Case against Regulating Encryption Technology», *Scientific American*, Vol. 279, No. 4, October 1998, pp. 116-117.

SAMET, H. and SOFFER, A. (1995): «A Map Acquisition, Storage, Indexing, and Retrieval System» in *Proceedings of the Third International Conference on Document Analysis and Recognition (ICDAR '95)*, Montréal, Canada, August 1995.

SCHNEIER, B. (1996): «*Applied Cryptography*», John Wiley & Sons, 1996.

TSUDIK, G. (1992): «Message Authentication with One-Way Hash Functions», *ACM Computer Communication Review*, Vol. 22, No. 5, 1992.

URECHE, O. et PLAMONDON, R. (1996): «Système électronique de transfert numérique de valeur: étude de faisabilité», *Éditions É.P.M.*, EPM/RT-96/22, 1996.

URECHE, O. et PLAMONDON, R. (1998a): «Module de facturation sécuritaire», *Éditions É.P.M.*, EPM/RT-98/02, 1998.

URECHE, O. and PLAMONDON, R. (1998b): «Digital Payment Systems for Internet Commerce – The State of the Art», soumis pour publication.

URECHE, O. et PLAMONDON, R. (1999a): «Module de facturation sécuritaire – Manuel d'utilisation», *Éditions É.P.M.*, EPM/RT-99/02, 1999.

URECHE, O. and PLAMONDON, R. (1999b): «Document Transport, Transfer and Exchange: Security and Commercial Aspects», in *Proceedings of the Fifth International Conference on Document Analysis and Recognition (ICDAR '99)*, IEEE Computer Society, Bangalore, India, 20-22 September 1999, pp. 585-588.

URECHE, O. et PLAMONDON, R. (1999c): «Paiements sur l'Internet», *Pour la science* – édition française de *Scientific American*, No. 260, juin 1999, pp. 45-49.

YOUNG, R. K. (1991): «*Wavelet Theory and its Applications*», Kluwer Academic Publishers, 1991.

ZHOU, J. and LOPRESTI, D. (1997): «Extracting Text from WWW Images», in *Proceedings of the 4th International Conference on Document Analysis and Recognition (ICDAR '97)*, Ulm, Germany, August 1997.

ZIMMERMANN, P. R. (1998): «Cryptography for the Internet», *Scientific American*, Vol. 279, No. 4, October 1998, pp. 110-115.

Références électroniques:

[AMZN] Amazon.com	http://www.amazon.com
[BWAR] Business Week Archives	http://bwarchive.businessweek.com
[FGEC] A Framework for Global Electronic Commerce	http://www.ecommerce.gov/framewrk.htm
[KRBR] Kerberos	http://www.rsa.com/rsalabs/faq/html/5-1-6.html
[PCMC] Politique cadre en matière de cryptographie aux fins du commerce électronique	http://strategis.ic.gc.ca/crypto
[RFCD] RFC DataBase, InterNIC	ftp://rs.internic.net
[SSLP] Protocole SSL	http://www.rsa.com/rsalabs/faq/html/5-1-2.html

Références des systèmes électroniques de paiement sur Internet:

ACC (Anonymous Credit Cards)	ftp://ftp.research.att.com/dist/anoncc/anoncc.ps.Z
AIMP (Anonymous Internet Mercantile Protocol)	http://ganges.cs.tcd.ie/mepeirce/Project /Oninternet/accinet.ps
BankGate WebWallet	http://www.bankgate.com/market/shopper
BankNet	http://mkn.co.uk/bank
Belle Systems A/S	http://www.belle.dk/micropay.html
BlueMoney	http://www.bluemoney.com
Brands, S.	http://www.cwi.nl/ftp/brands/e-cash.ps
BuyWay	http://clubweb.mpactimmedia.com
Camenisch, J., Piveteau, J.-M. & Stadler, M.	http://www.inf.ethz.ch/personal/camenisc

Chan, A., Frankel, Y. & Tsiounis, Y.	http://www.ccs.neu.edu/home/yiannis/papers/EC98.ps
Checkfree	http://www.checkfree.com
ClearCommerce	http://www.outrech.com
Clickshare	http://www.clickshare.com/clickshare
CommerceXpert (Netscape)	http://www.netscape.com/products/commapps/
Cybank	http://cybank.net
CyberCash	http://www.cybercash.com
CyberCoin	http://www.cybercash.com
DigiCash	http://www.digicash.com
eCHARGE	http://www.echarge.com
E-Check (FSTC)	http://www.fstc.org/projects/echeck
E-money.NET	http://www.e-money.net
eVend	http://www.evend.com
Ferguson, N.	ftp://ftp.cwi.nl/pub/CWIreports/AA/CS-R9318.ps.Z
First Virtual Holdings Inc.	http://www.fv.com
FOLC (Fair Off-Line e-Cash)	http://www.ccs.neu.edu/home/yiannis/papers/folc.ps
GlobeID – GTech	http://www.gctech.fr
GlobeSet	http://www.globeset.com
i-bill Web900	http://www.logicon.com/900.html
ICVerify, Inc	http://www.icverify.com
iKP	http://www.zurich.ibm.com:80 /Technology/Security/extern/ecommerce/iKP.html
InterCoin	http://www.intercoin.com
Internet Dollar	http://internetdollar.com
Klebox	http://www.klebox.com, http://kleline.fr
Lysyanskaya, A. & Ramzan, Z.	http://therory.lcs.mit.edu/~zulfikar
Magic Money	ftp://ftp.u.washington.edu /public/phantom/cpunk/mgmny.html
MicroMint	http://www.infosys.tuwien.ac.at/staff/rh/mimi/mimi.html
MilliCent (DEC)	http://www.MilliCent.com
MiniPay (IBM)	http://www.hrl.il.ibm.com/mpay
MPTP (Micro Payment Transfer Protocol)	http://www.w3.org/pub/WWW/TR/WD-mptp
Mondex	http://www.mondex.com
Neosphere Web TollBooth	http://www.neosphere.com
NetBill	http://www.netbill.com

NetCard	http://www.cl.cam.ac.uk/users/cm213/Project/
NetCash	http://www.teleport.com/~netcash
NetCheque	http://www.netcheque.com
NetChex	http://www.netchex.com
Net.Commerce (IBM)	http://www.software.ibm.com/commerce/net.commerce/
NetFare	http://www.netfare.com
OnLine Check	http://www.onlinecheck.com
OpenMarket	http://www.openmarket.com
Open Trading Protocol (OTP)	http://www.otp.org
Payline	http://www.payline.com
PayMe	http://ntrg.cs.tcd.ie/mepierce /Project/Payme/Overview.html
PayNow	http://www.cybercash.com
PayWord	http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps
Pay2See	http://www.pay2see.com
PC Pay	http://www.innovonics.com/pcpay
Quick-Checks	http://www.quick-checks.com
Redi-Check	http://www.redi-check.com
Safe Purchase	http://www.safepurchase.com
Secure-Bank.com	http://www.secure-bank.com
SecureBuy (AT&T)	http://www.att.com/work-net/securebuy/
Secure Electronic Transaction (SET)	http://www.set.com
SecureLink	http://www.openmarket.com
SecureOrder	http://www.atsbank.com
Secure Pay	http://www.anacom.co/payment.htm
SecureProcess	http://www.atsbank.net/ats-sp.htm
SecureTrans	http://www.securetrans.com
SecureWeb Payments - Terisa	http://www.terisa.com/products
SG2-Payline	http://www.sg2.fr/
SOX	http://www.systemics.com/docs/sox/execsummary.html
SNPP	ftp://allspice.lcs.mit.edu/pub/snpp/snpp-paper.ps
SubScrip	http://www.cs.newcastle.edu.au /Research/afurche/subscrip.ps
SuperCharge	http://super-charge.com
SVP	ftp://ftp.ens.fr/pub/reports/liens/liens-94-4.A4.ps.Z

TouchLink	http://touch.com
TRANZIX	http://www.scribens.polymtl.ca/tranzix/demo
VeriFone	http://www.verifone.com
Viaweb	http://www.viaweb.com
Vishnu (Wenbo Mao, Hewlett-Packard)	http://www.hpl.hp.co.uk/projects/vishnu/main.html, http://wenbomao.hpl.hp.com
WebCash	http://webcash.galaxy-net.net
WebCharge	http://www.webcharge.com
ZipLock	http://www.portsoft.com

[AIRR] Autres informations et recherches relevantes:

CyberSource	http://www.cybersource.com
E-Gold	http://www.e-gold.com
EIPaN	http://www.ict.tu-wien.ac.at/eipan
LETSystem	http://www.gmlets.u-net.com
TrefPunt	http://www.tref/nl/betalen
Wave	http://www.wave.com

ANNEXES

Afin de faciliter la compréhension du fonctionnement de base de notre système transactionnel, nous avons jugé utile d'ajouter deux annexes à cet ouvrage pour présenter en images le fonctionnement du prototype expérimental squelettique que nous avons réalisé, en montrant les deux applications concrètes décrites dans le Chapitre 5, à la section 5.2. Ces démonstrations simulées se trouvent également sur le site du système TRANZIX.

La première annexe présente une démonstration virtuelle d'une application permettant le contrôle des ressources physiques. Concrètement, l'application permet de contrôler l'impression à l'intérieur d'un intranet à l'aide d'un «Centre d'impression». Les usagers doivent être munis du logiciel de facturation sécuritaire, d'un fureteur ainsi que de plusieurs billets (ou jetons) leur permettant de payer les coûts d'impression de leurs documents.

La deuxième annexe présente une démonstration virtuelle d'une application permettant le contrôle d'accès à des ressources virtuelles, notamment à des images numériques. À l'aide d'un site Web servant de magasin virtuel, un vendeur peur offrir des images électroniques de cartes (dans notre exemple) ou toute autre information

binaire pouvant être acheminée numériquement à l'acheteur par l'intermédiaire de l'Internet.

Notons tout d'abord quelques aspects généraux. Les outils nécessaires pour utiliser ces applications sont les suivants:

- Le logiciel de facturation TRANZIX proprement dit;
- Le logiciel d'application d'impression (seulement pour l'application de contrôle des ressources physiques présentée dans l'Annexe I);
- Un interpréteur Java – version 1.1.3 ou plus récente;
- Un fureteur;

De plus, pour ouvrir un magasin virtuel, il est nécessaire d'avoir:

- Le système d'opération Linux 2.* ou Solaris 2.* (les scripts CGI en format `.bat` pour Windows 95, 98 ou NT ne sont pas disponibles présentement);
- Un serveur Web compatible avec le standard HTTP 1.0;
- Les scripts servant d'intermédiaire entre le serveur Web et le logiciel de facturation sécuritaire TRANZIX ainsi que les scripts permettant de contrôler les applications proprement dites;
- Le gestionnaire des fichiers reçus pour impression (seulement pour l'application de contrôle des ressources physiques présentée dans l'Annexe I).

ANNEXE I

EXEMPLE DE CONTRÔLE DES RESSOURCES PHYSIQUES

Une fois rendu à l'aide de son fureteur dans le magasin virtuel du «Centre d'impression» (Fig. A.1.1), l'acheteur peut cliquer sur le lien payant. Dans notre exemple, le prix d'impression est directement proportionnel à la grandeur, exprimée en octets, du fichier à imprimer – et tient ainsi compte autant de la quantité d'encre consommée que de la quantité de papier utilisée.

En même temps, l'acheteur doit déjà avoir démarré l'application d'impression IMPRIMEUR (Fig. A.1.2), avant de poursuivre. Cette application, qui ne relève pas du logiciel de facturation ni du système TRANZIX, sert seulement à l'envoi électronique du document de l'ordinateur de l'acheteur au centre d'impression. De cette façon, le magasin virtuel peut établir de manière interactive le prix demandé à l'acheteur, en mesurant la grandeur du fichier envoyé. Une fois démarré, l'IMPRIMEUR attend la connexion avec le centre d'impression.

Après avoir pris la décision d'imprimer, l'acheteur suit le lien payant. Par l'intermédiaire de l'interface du serveur Web du magasin, le centre d'impression tentera une connexion avec l'application d'impression IMPRIMEUR de l'acheteur; dès que cette connexion est réalisée, l'IMPRIMEUR demande à l'usager d'entrer le nom du fichier qu'il

désire imprimer (Fig. A.1.3) – (dans cet exemple, le fichier "Document.ps"). Après avoir entré le nom du document à imprimer, le fichier – s'il existe et s'il est trouvé – est envoyé au centre d'impression. Sinon, un message d'erreur est affiché (Fig. A.1.4) et l'usager devra entrer de nouveau le nom du fichier – avec son chemin complet.

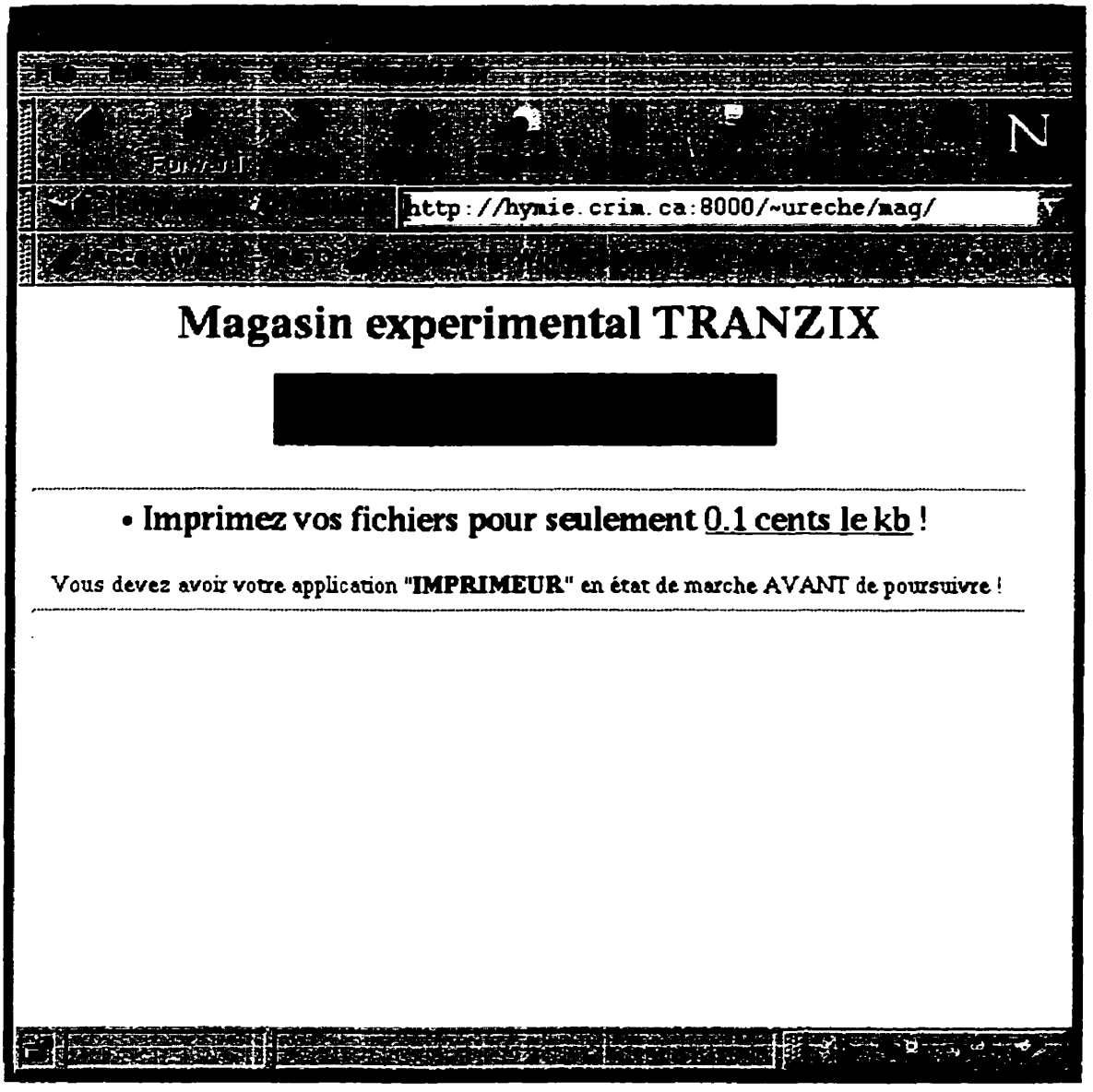

Figure A.1.1 – *Exemple simplifié de magasin virtuel: le «Centre d'impression»*

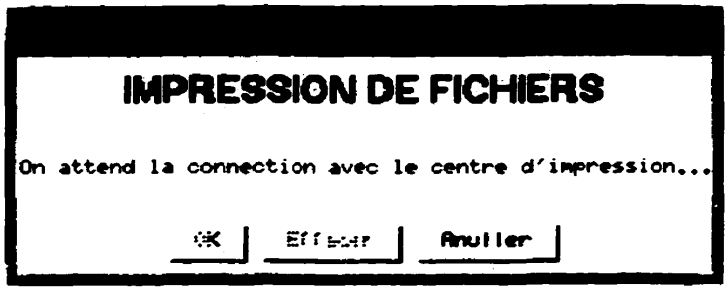

Figure A.1.2 – *L'application d'impression* IMPRIMEUR *en attente*

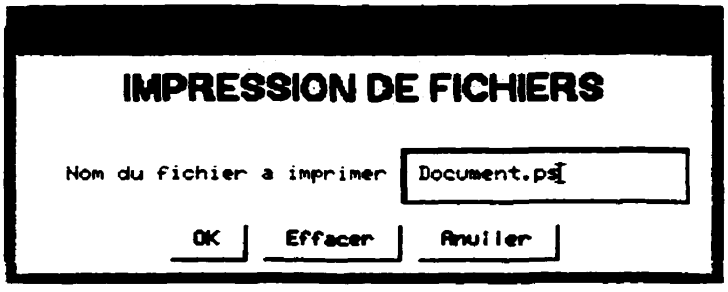

Figure A.1.3 – *L'application d'impression* IMPRIMEUR *avant l'envoi du fichier à imprimer*

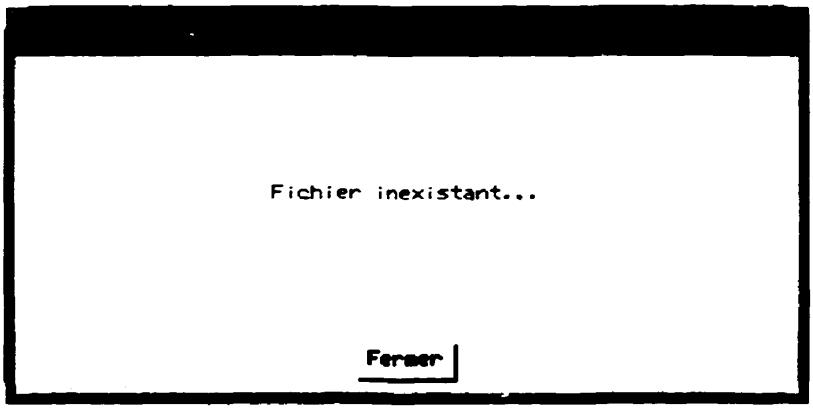

Figure A.1.4 – *Message d'erreur affiché par l'application d'impression*

Une fois le transport du fichier complété, l'acheteur est invité à poursuivre la transaction (Fig. A.1.5) à l'aide de son fureteur. La partie serveur de l'application

d'impression (le script `interface.cgi`) calcule le prix de l'impression, il l'écrit dans un fichier protégé pour pouvoir le comparer avec la requête à recevoir – si le client accepte de payer – et il construit dynamiquement une page réponse (Fig. A.1.6) qui sera affichée comme résultat de la requête de transaction de l'acheteur. Le prix exact correspondant à la quantité d'information contenue dans le fichier à imprimer est affiché, suivi par le lien payant qui permet de déclencher le démarrage du module de facturation sécuritaire TRANZIX de magasin virtuel.

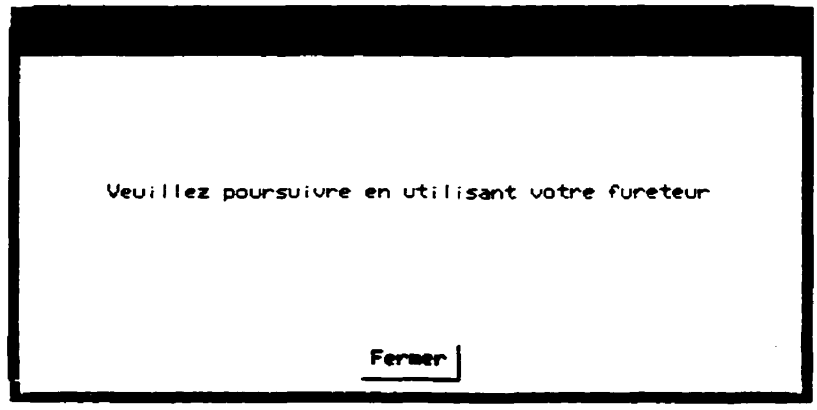

Figure A.1.5 – *Message pour indiquer la poursuite de la transaction*

Cette étape supplémentaire dans le flux transactionnel est nécessaire afin de permettre au centre d'impression d'établir dynamiquement un prix, en fonction de la grandeur de chaque document à imprimer. Si cette étape n'avait pas été ajoutée, le centre d'impression aurait dû, par exemple, demander un prix fixe pour tous les documents, sans tenir compte de leur grandeur.

À ce stade-ci, l'acheteur a le choix d'accepter le prix demandé par le centre d'impression et de poursuivre en cliquant sur le lien payant dans la page réponse ou de refuser et de sortir du centre d'impression. Dans ce cas, la copie de son fichier présente sur le serveur du centre d'impression est effacée.

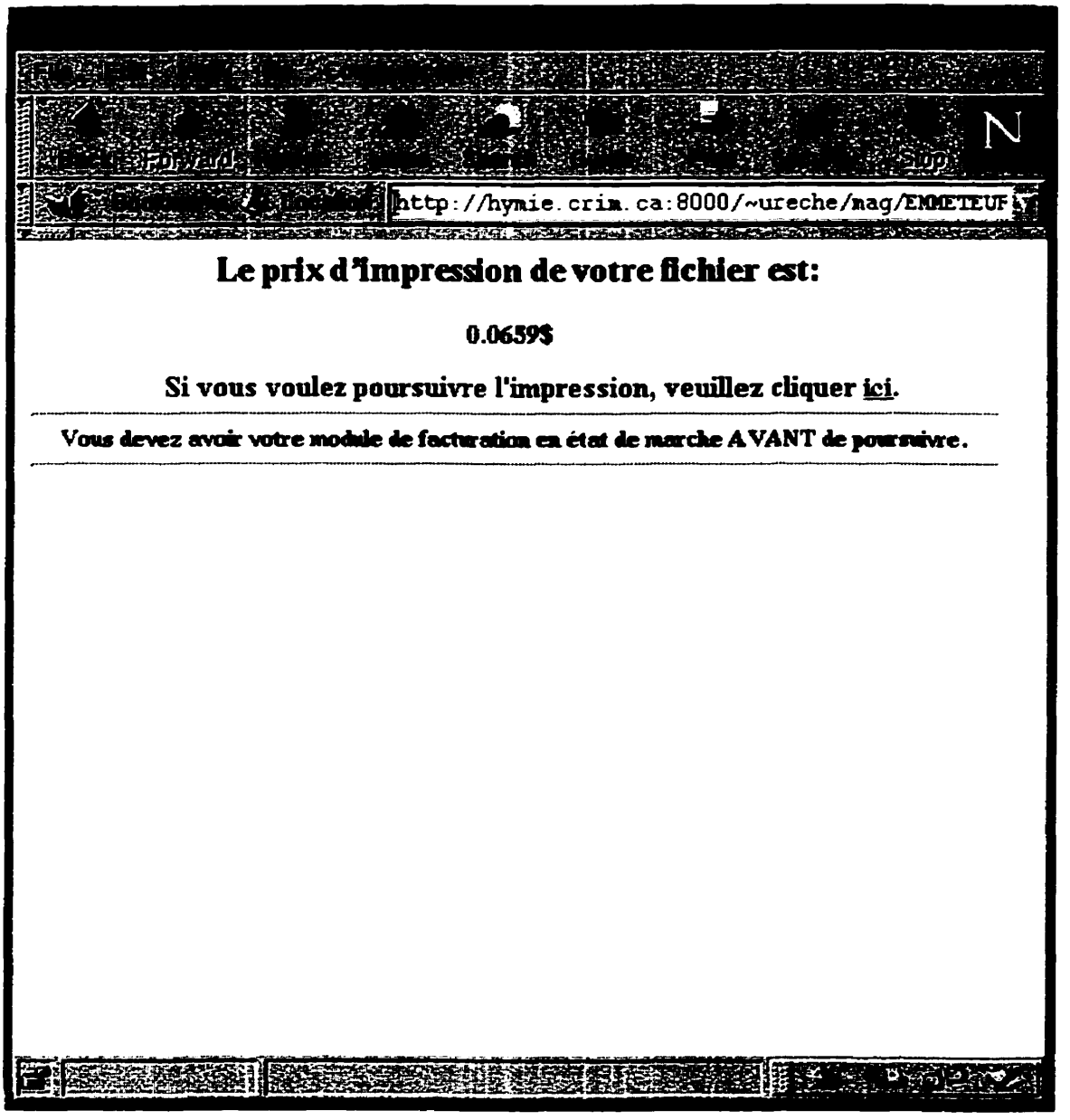

Figure A.1.6 – *Page dynamique de réponse contenant le prix à payer*

S'il décide d'accepter, son logiciel de facturation doit être démarré avant de poursuivre le lien payant. En poursuivant ce nouveau lien payant, l'acheteur démarre l'interface qui sert d'intermédiaire entre le serveur Web du magasin virtuel et le logiciel de facturation sécuritaire TRANZIX du vendeur. Ainsi, l'interface déclenche le

démarrage du logiciel de facturation du centre d'impression, qui essaie de contacter le logiciel de facturation de l'acheteur pour lui envoyer une requête de paiement. Une fois la connexion établie, un court signal sonore est émis pour avertir l'acheteur de la réception d'une connexion et une fenêtre d'affichage s'affiche sur son écran (Fig. A.1.7). Il est ainsi avisé de la réception d'une requête de paiement. Le nom du vendeur, son adresse électronique, l'adresse Internet du magasin, le montant[1] ainsi qu'une description (facultative) de la transaction sont affichées.

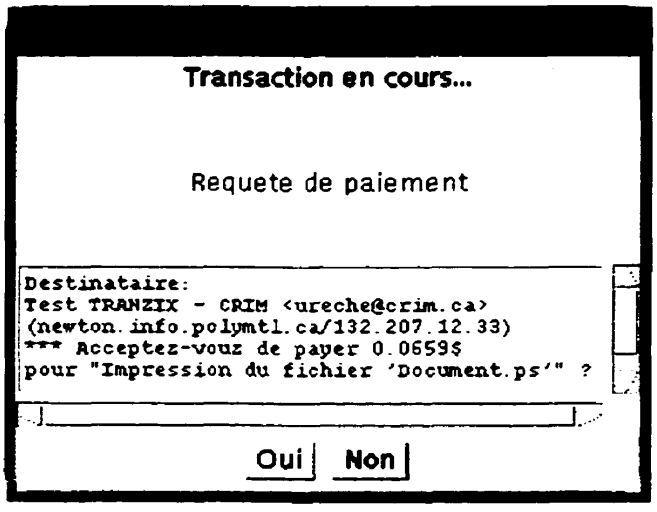

Figure A.1.7 – *Message de requête de paiement affiché par le logiciel de facturation*

L'acheteur aura la possibilité de refuser ou d'accepter le paiement. S'il refuse, la transaction échoue et une page d'échec est affichée (Fig. A.1.8) dans son fureteur. Une courte liste des raisons possibles de l'échec d'une transaction, ainsi qu'un espace contenant l'adresse de l'ordinateur de l'acheteur sont incluses dans cette page. Cette adresse peut être modifiée, si, par exemple, l'acheteur se trouve sur un autre ordinateur, ayant une adresse IP différente ou s'il est à l'arrière d'une passerelle de protection (*firewall*). Il n'aura alors qu'à rentrer l'adresse IP exacte et à cliquer "OK".

[1] Dans notre exemple, comme il s'agit d'un document d'une soixantaine de kilo-octets, il faut payer 6.59 cents ou 0.0659 $.

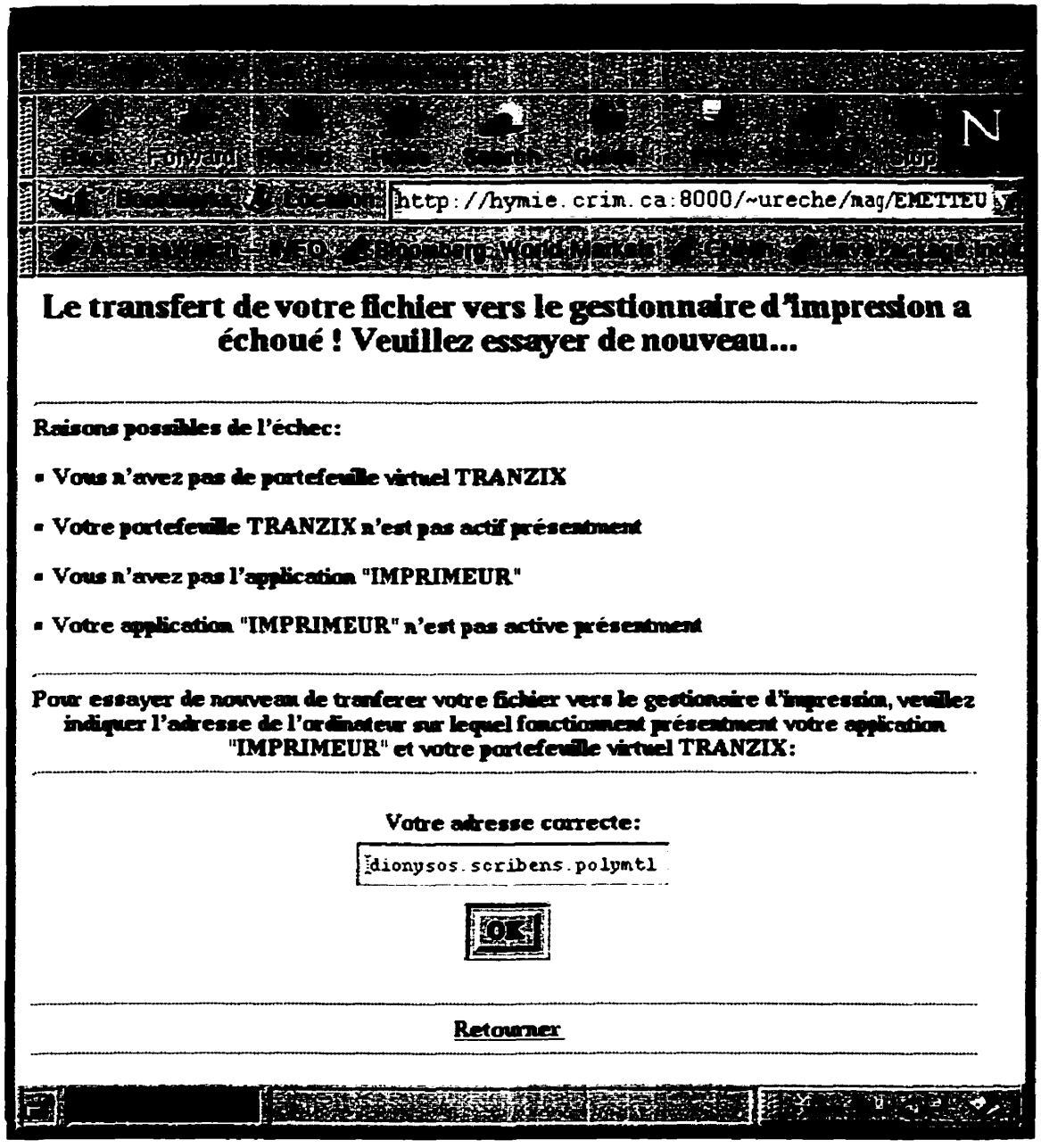

Figure A.1.8 – *Page d'échec*

S'il accepte, les deux logiciels commencent à exécuter les étapes du protocole transactionnel de facturation. Si la transaction est réussie, le module de facturation du vendeur, à l'aide du contrôleur d'application, envoie le document à

l'impression proprement dite et affiche, dans le fureteur de l'acheteur, une page résultat (Fig. A.1.9.) indiquant la réussite de la transaction ainsi que le nom de l'imprimante où le fichier a été envoyé pour impression. Il ne restera à l'acheteur qu'à aller chercher son document imprimé.

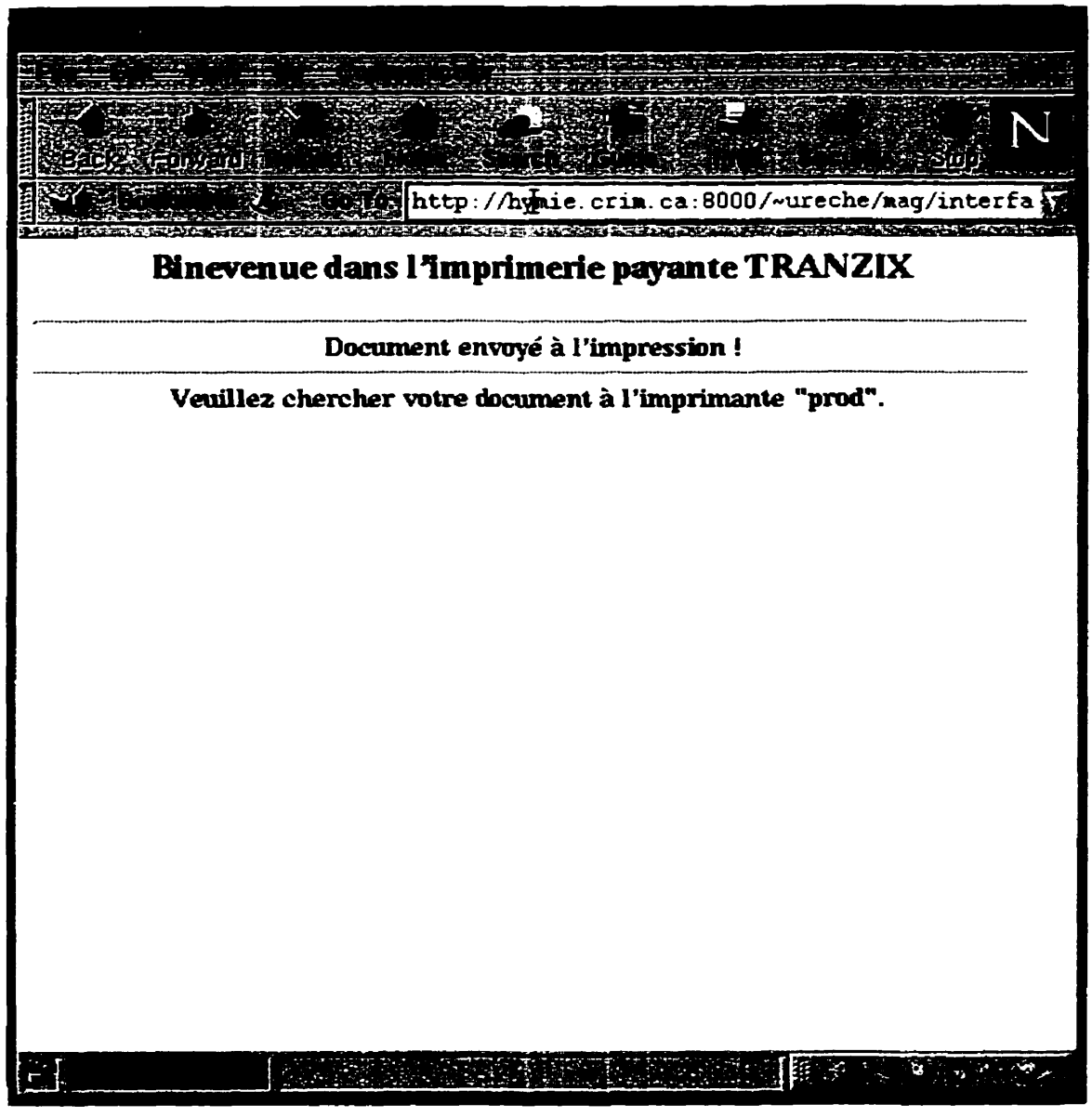

Figure A.1.9 – *Page résultat indiquant l'imprimante qui a effectué l'impression*

ANNEXE II

EXEMPLE DE CONTRÔLE D'ACCÈS À DES RESSOURCES VIRTUELLES

Cette application permet la vente numérique de produits ou de services virtuels. Elle fonctionne essentiellement de la même manière que l'application précédente – présentée dans l'Annexe I – sauf pour l'étape supplémentaire de transfert et d'évaluation dynamique du prix du fichier à imprimer, étape qui n'est plus nécessaire dans le cas présent.

L'acheteur arrive sur le site du magasin virtuel du vendeur, que nous avons appelé pour cet exemple «Le Cartographe Virtuel». Une fois rendu dans le magasin virtuel (Fig. A.2.1), il peut cliquer sur un lien payant. L'acheteur doit avoir son portefeuille virtuel en état de marche avant de poursuivre, tandis que le portefeuille virtuel du vendeur sera démarré par le serveur Web du magasin virtuel par l'intermédiaire de l'interface que nous avons déjà mentionnée au Chapitre 5.

En suivant le lien payant, l'acheteur envoie une requête de transaction qui déclenche le démarrage de l'interface qui sert d'intermédiaire entre le serveur Web du magasin et le portefeuille virtuel du vendeur. Ainsi, l'interface démarre le module de

facturation du vendeur, qui essaye de contacter le logiciel du client. Une fois la connexion établie, une requête de paiement est envoyée à l'acheteur.

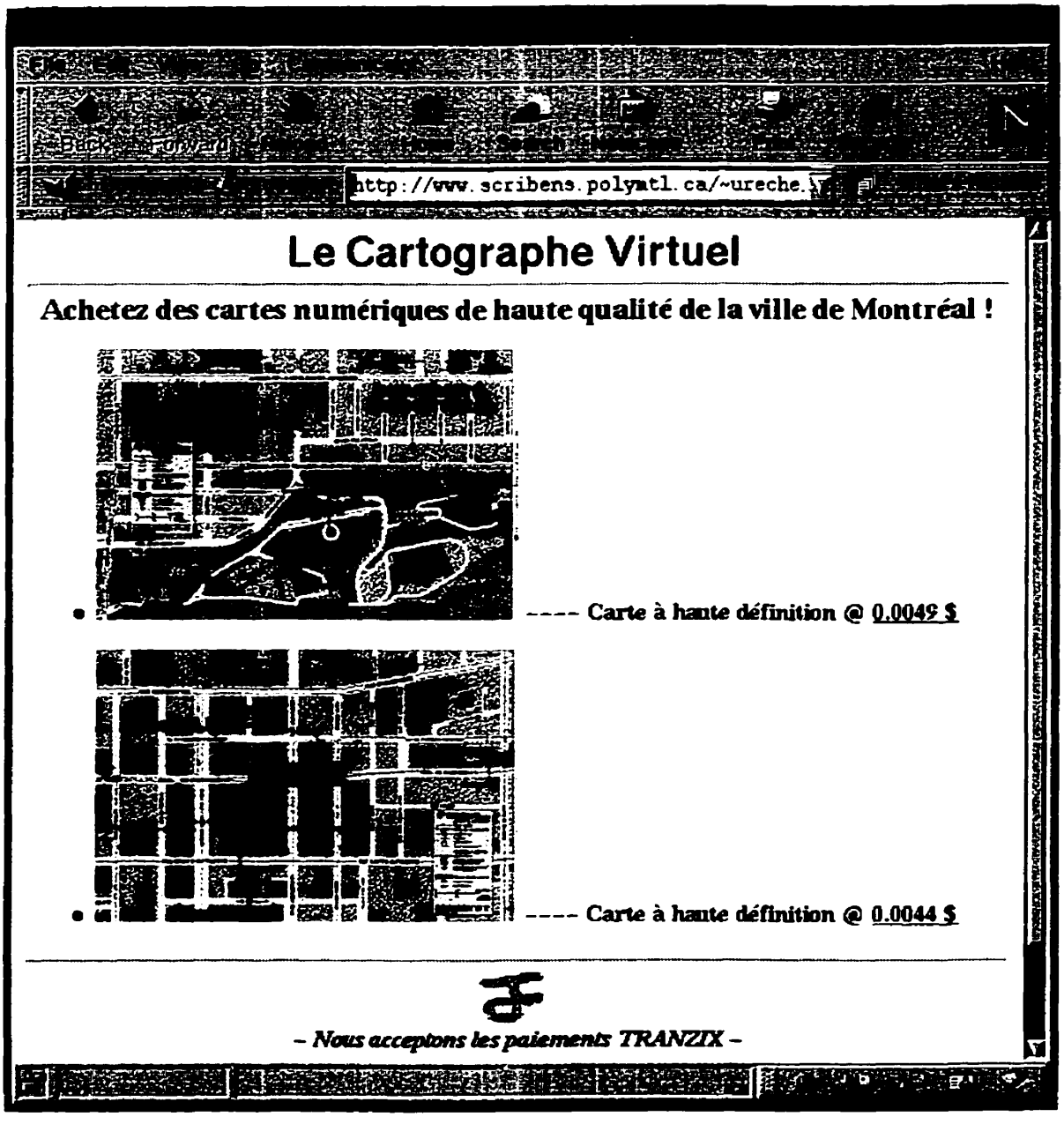

Figure A.2.1 – *Le cyber-magasin «Le Cartographe Virtuel»*

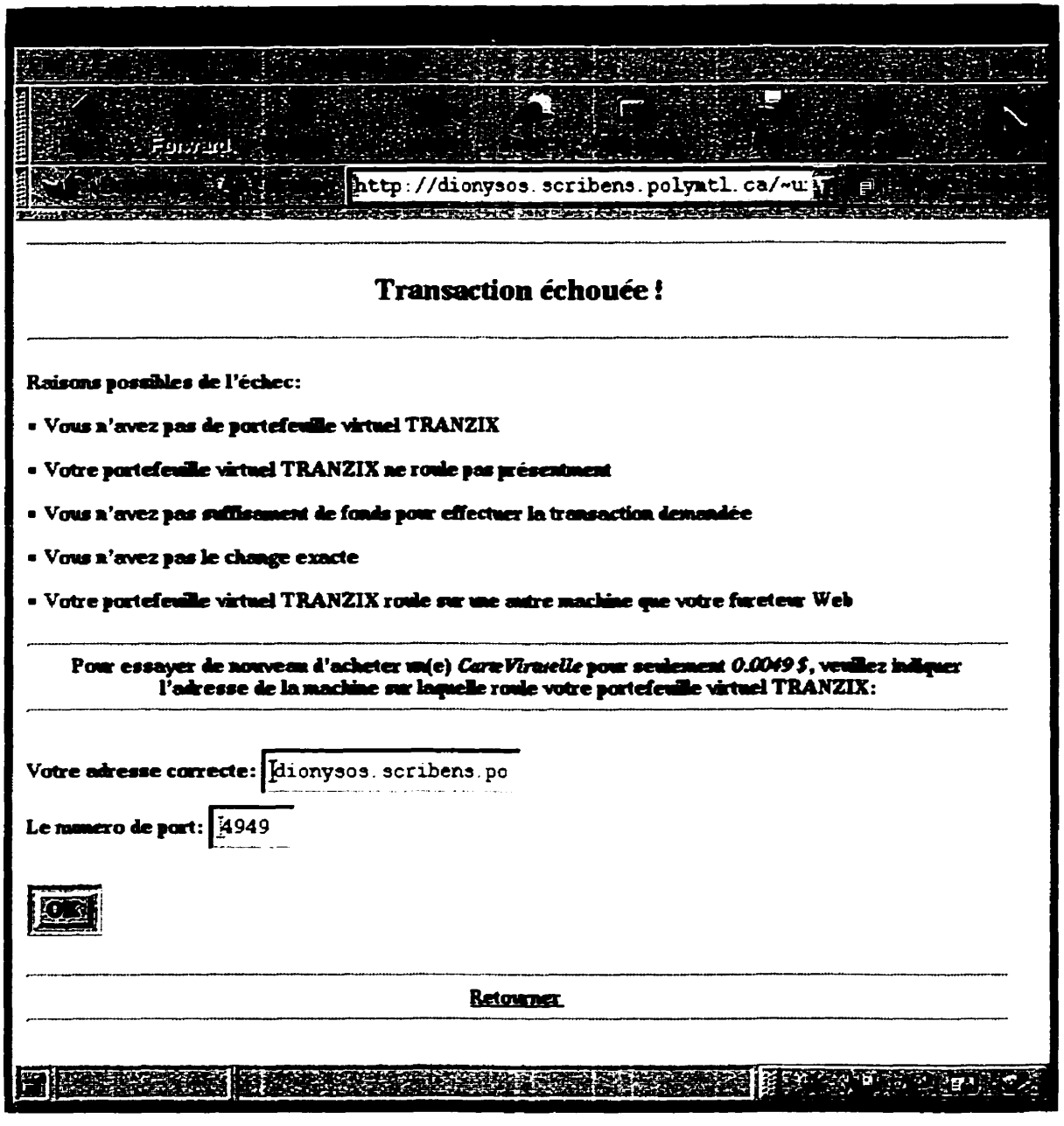

Figure A.2.2 – *Page d'échec construite dynamiquement*

Si la transaction ne peut pas avoir lieu pour une raison quelconque, une page d'échec est affichée (Fig. A.2.2). Cette page est construite dynamiquement, affichant le nom et le coût du produit qui devait être acheté. Tout comme dans l'exemple de

l'application précédente, cette page d'échec contient une courte liste des raisons possibles de l'échec, ainsi qu'un espace contenant l'adresse de l'ordinateur de l'acheteur. Cette adresse peut être modifiée, il n'aura qu'à rentrer l'adresse IP exacte et à cliquer "OK".

Par contre, si les deux logiciels peuvent se connecter, le logiciel de facturation sécuritaire du vendeur envoie une requête de paiement à l'acheteur; l'acheteur devra autoriser la transaction, plus précisément le paiement de la marchandise (Fig. A.2.3). Si l'acheteur refuse d'effectuer le paiement, la transaction prend fin. S'il accepte de payer, le paiement est effectué, le vendeur recevra le(s) billet(s) et enverra à l'acheteur un reçu virtuel signé numériquement ainsi que la marchandise – dans ce cas la page contenant l'image de la carte demandée.

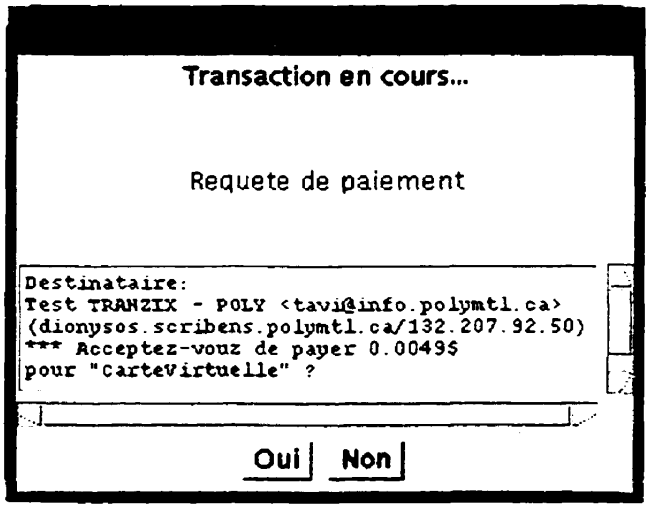

Figure A.2.3 – *Message de requête de paiement pour l'achat d'une image de carte affiché par le logiciel de facturation*

Une fois le paiement effectué, l'acheteur peut accéder à la page contenant l'image du timbre (Fig. A.2.4). Dans le cas des marchandises «réelles», cette page pourrait contenir le numéro d'envoi par la poste, courrier ou d'autres moyens de transport

physique. Notons que le répertoire dans lequel la «marchandise» est stockée sur le serveur Web du magasin est protégé contre les accès non-autorisés. Cette protection peut être réalisée soit à l'aide de scripts, soit directement à l'aide du serveur Web et de ses clauses de protection des répertoires.

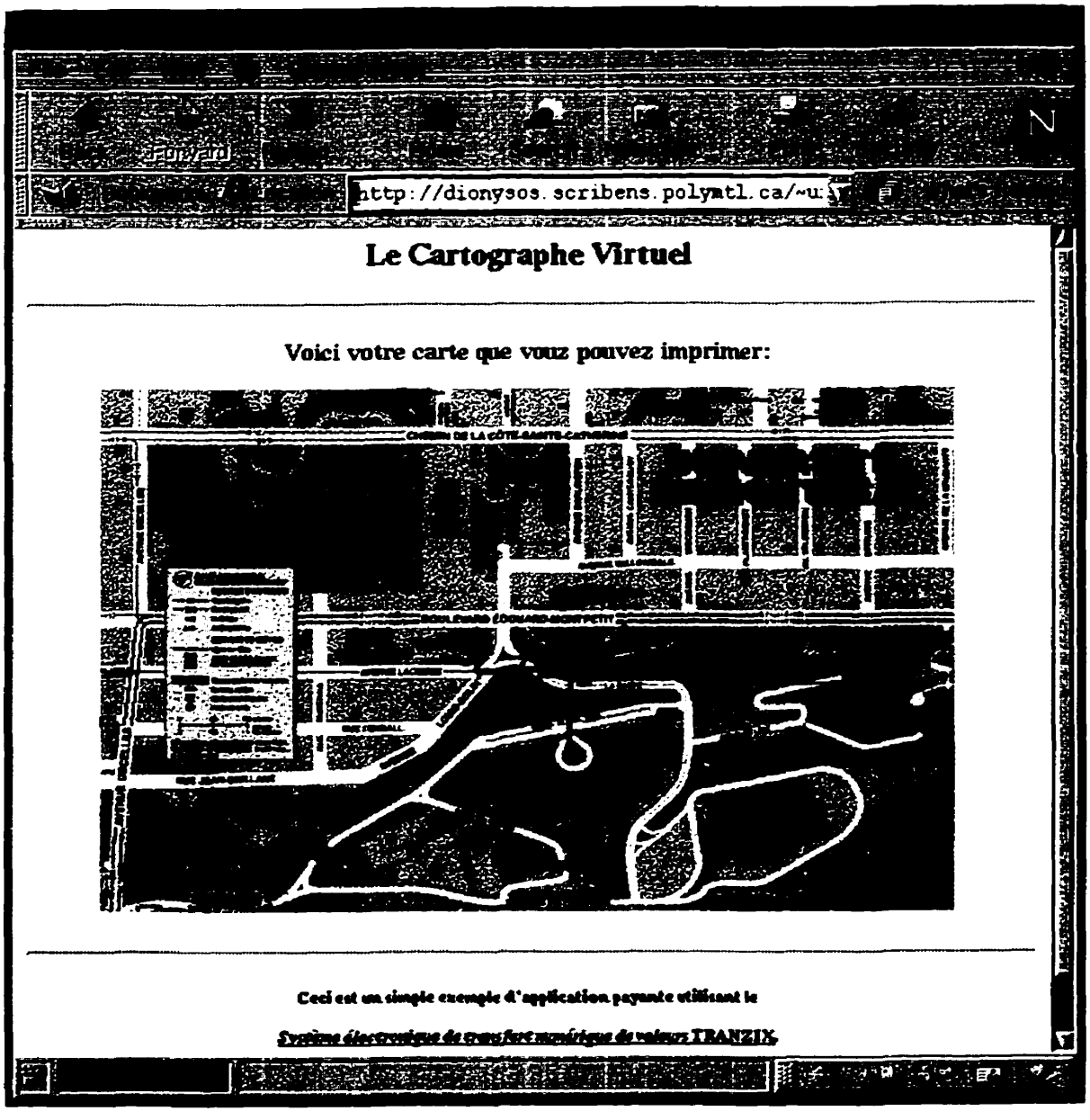

Figure A.2.4 – *La page contenant la marchandise – l'image du timbre*