CAHIER D'ÉTUDES
WORKING PAPER

N° 10

NOUVEAUX INSTRUMENTS DE PAIEMENT: UNE ANALYSE DU POINT DE VUE DE LA BANQUE CENTRALE

par Li-Chun YUAN
Novembre 2003

BANQUE CENTRALE DU LUXEMBOURG
EUROSYSTÈME

Address : 2, Boulevard Royal - L-2983 Luxembourg
Telephone : (+352) 4774 - 1
Fax : (+352) 4774 - 4901
Internet : http://www.bcl.lu
E-mail : sg@bcl.lu
Télex : 2766 IML LU

TABLE DES MATIERES

1 INTRODUCTION 5

2 PAIEMENTS ET SYSTÈMES DE PAIEMENT 6

2.1 DÉFINITIONS 6
2.1.1 LE PAIEMENT 6
2.1.2 LA MONNAIE ET LES MOYENS DE PAIEMENT 6
2.1.3 LES INSTRUMENTS DE PAIEMENT 7
2.1.4 LES SYSTÈMES DE PAIEMENT 8
2.1.4.1 Risques associés aux systèmes de paiement 9
2.1.4.2 Le risque systémique 10
2.1.5 EFFET DE RÉSEAU 11

2.2 CADRE LÉGAL ET RÉGLEMENTAIRE 11
2.2.1 LA LÉGISLATION LUXEMBOURGEOISE 12
2.2.1.1 Législation concernant le secteur bancaire 12
2.2.1.2 Législation favorisant le commerce électronique 14
2.2.2 LA LÉGISLATION EUROPÉENNE 15
2.2.2.1 Législation concernant le secteur bancaire et les paiements 15
2.2.2.2 Législation favorisant le commerce électronique 17
2.2.3 RÔLE DES AUTORITÉS ET DES BANQUES CENTRALES 19
2.2.4 RÔLE DU SYSTÈME EUROPÉEN DES BANQUES CENTRALES 21

3 LES NOUVEAUX INSTRUMENTS DE PAIEMENT 22

3.1 DÉFINITIONS 23
3.1.1 PAIEMENTS ÉLECTRONIQUES 23
3.1.2 LA MONNAIE ÉLECTRONIQUE 25
3.1.3 LES PAIEMENTS MOBILES 26
3.1.3.1 Identification 26
3.1.3.2 Pertinence des paiements mobiles 27
3.1.3.3 Exemples de solutions de paiement mobile 29
3.1.3.4 Caractéristiques et modèles 36
3.1.3.5 Cadre réglementaire 39
3.1.3.6 Incertitudes pour les paiements mobiles 41

3.2 SPÉCIFICITÉS DES INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE 41

3.3 RISQUES ASSOCIÉS AUX INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE 42

3.4 COMPOSANTES DE SÉCURITÉ DES INSTRUMENTS DE PAIEMENT 44
3.4.1 DISPONIBILITÉ 44
3.4.2 AUTHENTICITÉ 44
3.4.3 NON RÉPUDIATION 45
3.4.4 CONFIDENTIALITÉ 45
3.4.5 INTÉGRITÉ 45

4 FUTUR DES PAIEMENTS ÉLECTRONIQUES 45

4.1 CONDITIONS DE RÉUSSITE 45

4.2 AUTOMATISATION DE BOUT EN BOUT 46

4.3 INITIATIVES DES AUTORITÉS 46
4.3.1 INITIATIVES DES INSTITUTIONS EUROPÉENNES 46
4.3.2 INITIATIVES RÉCENTES DU SEBC ET DE LA BCE 47
4.3.3 INITIATIVES HORS UNION EUROPÉENNE 48

4.4 INITIATIVES DU MARCHÉ 48

4.5 LA SITUATION LUXEMBOURGEOISE 49

5 CONCLUSION 50

6 BIBLIOGRAPHIE 51

ANNEXE 1: STATISTIQUES INSTRUMENTS DE PAIEMENT 54

ANNEXE 2: RÉSEAUX DE COMMUNICATION SANS FIL 55

LA SECONDE GÉNÉRATION DE TÉLÉPHONIE MOBILE 55

ÉVOLUTION DES RÉSEAUX DE COMMUNICATION SANS FIL 55

TERMINAUX MOBILES EN TANT QUE TERMINAUX DE PAIEMENT 56

ANNEXE 3: SÉCURITÉ DES RÉSEAUX
DE COMMUNICATION SANS FIL 57

SUPPORT PHYSIQUE 57
LA CARTE A PUCE 57
LE SPECTRE RADIOÉLECTRIQUE 57

TECHNIQUES LOGICIELLES 57
GARANTIE DE L'AUTHENTICITÉ DES PARTIES 57
- Le mot de passe à usage unique 58
- La technique du défi-réponse (challenge) 58
GARANTIE DE L'INTÉGRITÉ ET/OU DE CONFIDENTIALITÉ 58
Les systèmes symétriques 58
Les systèmes asymétriques 59
- Secure Socket Layer 60
- Secure Electronic Transaction 60
- PKI sans fil 60

1 Introduction

Les évolutions technologiques apportent des solutions de paiement de détail innovantes (paiements par téléphone mobile par exemple). Afin de décider si ces dernières sont qualifiables de nouveaux instruments de paiement, le présent document commencera par une analyse basée sur la définition des différentes formes de monnaie (dont la monnaie électronique) et des instruments de paiement. Ces solutions seront aussi considérées dans leur cadre plus général des paiements et des systèmes de paiement, ainsi que dans leur contexte réglementaire national et européen.

Parmi les nouvelles possibilités technologiques, l'on peut distinguer les systèmes de téléphonie mobile car ils offrent des atouts techniques et commerciaux pour le développement de solutions de paiements mobiles d'ambition ubiquitaire. Comme pour certaines solutions électroniques de paiement de détail, les paiements mobiles sont l'occasion pour des entrepreneurs non liés au secteur bancaire de devenir des prestataires de paiement de masse. L'observation des caractéristiques et des modèles de solutions de paiement électroniques et mobiles nous permettra d'identifier si cette participation tend à être coopérative ou concurrentielle avec les banques.

S'agissant des paiements, la garantie de sécurité est primordiale aux yeux des utilisateurs. D'autant plus que l'utilisation de réseaux de télécommunication ouverts (la téléphonie mobile, Internet, etc.) génère des craintes supplémentaires liées à la fraude et à la sécurité. Aussi, une partie du document sera consacrée aux risques associés aux paiements électroniques et à leurs composantes de sécurité.

Finalement, nous aborderons différentes initiatives publiques et privées qui ont pour but de promouvoir la sécurité et l'efficience des paiements électroniques. Nous verrons que parmi les autorités monétaires, le Système européen des banques centrales est assez entreprenant en la matière.

2 Paiements et systèmes de paiement

2.1 Définitions

2.1.1 Le paiement

Le Petit Robert définit le terme "paiement" de la manière suivante: "Ce qu'on donne pour exécuter une obligation, et qui éteint cette obligation". Par exemple, dans notre économie, la dette contractée lors d'un achat est une obligation qui peut être éteinte par un paiement. Dans le langage courant, le paiement sert à éteindre une dette d'argent.

La définition de "paiement" de la Banque des Règlements Internationaux[1] (BRI), est d'une orientation plus monétaire: "transfert de la créance monétaire par le payeur à une partie acceptable au bénéficiaire". Elle est partagée par la Banque centrale européenne (BCE)[2].

Lorsque le paiement s'effectue au moyen de billets de banque et de pièces de monnaie ayant cours légal, la créance du créditeur sur le débiteur est transférée sur l'Etat. C'est un paiement fiduciaire.

De manière similaire, lorsque le débiteur effectue le paiement par virement bancaire, la créance du créditeur sur le débiteur se change en créance du créditeur sur sa banque. On parle alors de paiement scriptural.

Dans les deux cas, il y a effectivement transfert de créance. En acceptant un tel transfert, le créancier témoigne de sa confiance respectivement en les signes monétaires et en sa banque.

Les paiements dont il sera question tout au long de ce document sont les paiements de masse (ou de détail), et en corollaire les instruments de paiement de masse et les systèmes de paiement de masse.

Selon la BRI[3], les paiements de masse se caractérisent par:
1. Un nombre élevé de transactions
2. Un montant relativement faible de chaque transaction
3. Un nombre élevé de contreparties (consommateurs et entreprises)
4. Un grand nombre d'instruments

2.1.2 La monnaie et les moyens de paiement

La monnaie sert communément au paiement, l'usage que nous en faisons tous les jours en est la preuve. En cela, la monnaie est un outil servant aux échanges. Là n'est pas la seule fonction de la monnaie:
- Elle est une unité de compte (la valeur d'un bien s'exprime en unités monétaires);
- Elle est une réserve de valeur (les unités monétaires peuvent être conservées pour un usage futur).

---

[1] BRI - BIS, Committee on Payment and Settlement Systems, A glossary of terms used in payments and settlement systems, January 2001, revised July 2001
[2] BCE - ECB, Blue Book Payment and securities settlement systems in the European Union, Annex 4: Glossary, June 2001
[3] BRI - BIS, Committee on Payment and Settlement Systems, Retail Payments in Selected Countries: A Comparative Study, September 1999

La monnaie existe sous la forme de signes monétaires, les billets de banque et les pièces métalliques. C'est la monnaie fiduciaire.

Le terme "monnaie" recouvre aussi les fonds déposés sur le compte d'un établissement de crédit. Dans ce cas, on parle de monnaie scripturale.[4]

La monnaie scripturale et la monnaie fiduciaire servent à la réalisation de paiements. De par cette fonction, ce sont des moyens de paiement.

2.1.3 Les instruments de paiement

Un moyen de paiement ne suffit pas de lui-même à effectuer un paiement ou à transférer des fonds. On peut dès lors définir un instrument de paiement comme un instrument[5] qui permet de transférer des fonds sans restriction ni définition quant au support ou à la technologie utilisée à cet effet. Un instrument de paiement consiste en l'instruction de transfert liée au système qui en permet la communication pour traitement[6]. Les instruments de paiement permettent donc la circulation de la monnaie et les paiements.

Les instruments de monnaie fiduciaire sont les billets de banque et les pièces de monnaie.

Les instruments de paiements scripturaux sont plus nombreux: chèques, virements, débit direct, cartes de crédit, cartes de débit, effets de commerce...[7]

Tant les instruments de monnaie fiduciaire que les instruments de paiement scripturaux sont des instruments de paiement. Néanmoins, leurs contextes d'utilisation et leurs fondements diffèrent.

En effet, la loi confère une particularité importante, le cours légal[8], aux billets et aux pièces. Ces derniers constituent ainsi la monnaie légale, avec les conséquences suivantes:

1. L'acceptation des billets et des pièces est obligatoire;
2. Le signe monétaire est comptabilisé (et doit être accepté) pour sa valeur faciale;
3. Le signe monétaire a un pouvoir libératoire, son transfert a pour conséquence l'extinction immédiate de la créance à hauteur de sa valeur nominale. Le pouvoir libératoire est cependant limité pour les pièces[9];
4. Le porteur du signe monétaire peut exiger son remboursement sous forme de métal précieux ou sous forme d'autre signe ayant cours légal. Néanmoins cette possibilité est rendue caduque par l'instauration du cours forcé qui rend la monnaie inconvertible par rapport au métal précieux.

En principe, le créancier a donc toujours le droit d'exiger un paiement fiduciaire.

---

[4] Les billets de banque et les pièces de monnaie en circulation constituent l'agrégat monétaire M0.
M0 correspondait à 7% de M3 (l'offre de monnaie totale) dans la zone euro, BCE 5/99, cité par Birch David, E-money and Payment Systems Review, Retail electronic payments, Central Banking Publications, 2002

[5] BCE - ECB, Blue Book Payment and securities settlement systems in the European Union, Annex 4: Glossary, June 2001

[6] Kuttner Kenneth N. and McAndrews James J., FRBNY Economic Policy Review, Personal On-Line Payments, December 2001

[7] Voir Annexe 1 pour une comparaison statistique européenne entre instruments de paiement.

[8] Articles 17 à 20 de la loi organique de la Banque centrale du Luxembourg.
Article 106 (ex-article 105 A) du Traité instituant la Communauté européenne.

[9] Article 20 de la loi organique de la Banque centrale du Luxembourg.
Article 11 du règlement du Conseil n° 974/98 du 3 mai 1998 concernant l'introduction de l'euro.

D'autres caractéristiques différencient les deux sortes de monnaie. La monnaie fiduciaire:
- Ne nécessite pas d'instruction ni de système de communication spécifiques. La transmission physique suffit;
- Est de transmissibilité immédiate, elle est immédiatement réutilisable par son porteur;
- Ne nécessite pas la détention d'un compte auprès d'un établissement de crédit;
- Se compense et se liquide d'elle-même;
- Est limitée aux transactions face-à-face;
- Assure l'anonymat des porteurs et des transactions.

Alors que pour les instruments scripturaux,
- L'inscription d'une transaction et sa communication pour traitement sont requises;
- Une inscription en compte est obligatoire avant toute utilisation;
- L'identité du titulaire du compte est connue;
- Le règlement passe par l'intermédiaire d'un système de compensation et de règlement (exception faite du cas où le débiteur et le créditeur ont un compte auprès de la même institution);
- Des contextes multiples d'utilisation sont possibles: transactions face à face, commerce à distance, opérations transfrontalières…
- Les transactions doivent pouvoir être retracées, notamment pour des raisons de sécurité.

Le niveau de sécurité tel qu'il est perçu par les consommateurs est justement un paramètre clé pour l'acceptation d'instruments de paiement, car ceux-ci touchent directement à l'argent et à la monnaie. En ce qui concerne la monnaie fiduciaire, le risque principal est le faux monnayage contre lequel les billets et les pièces sont protégés par des mesures de sécurité physiques (poids, filigrane, fil de sécurité, hologrammes…).

Etant donné les contextes variés d'emploi la monnaie scripturale, il importe lors d'une transaction:
- D'identifier et d'authentifier les parties en présence;
- De vérifier la validité de l'instrument;
- De garder certains éléments confidentiels et de prévenir toute interception par une partie indésirable, à tout moment;
- De maintenir intacts tous les paramètres identifiant la transaction.

Ce sont les composantes de sécurité qui font l'objet d'une politique de sécurité et de lutte contre la fraude, comme nous le verrons dans le paragraphe Composantes de sécurité des instruments de paiement.

2.1.4 Les systèmes de paiement

Les paiements scripturaux s'effectuent souvent entre comptes bancaires détenus auprès d'institutions différentes. Le transfert de fonds doit alors passer par un système de paiement interbancaire. Un système de paiement est défini comme un ensemble d'instruments, de méthodes et de règles permettant le transfert de fonds entre ses participants. Les systèmes de paiement revêtent donc une importance fonctionnelle en permettant un traitement efficace des paiements et des règlements. Ils contribuent ainsi au bon fonctionnement d'une économie de marché moderne.

Les systèmes de paiement sont nombreux et de différentes catégories. Leurs paramètres distinctifs sont:

- Le traitement de paiements de masse ou de gros montants;
- Le traitement en temps réel ou en différé;
- Le règlement après compensation ou en montants bruts;
- L'actif de règlement.

Tenant compte de l'importance économique des systèmes de paiement et de leur complexité, il est nécessaire de s'assurer de leur bon fonctionnement. A cette fin, une bonne connaissance de leurs risques potentiels est utile.

2.1.4.1 Risques associés aux systèmes de paiement

1. Risque de crédit
Le risque qu'un participant au système soit incapable d'acquitter intégralement ses obligations financières au sein du système, au moment prévu ou ultérieurement.

2. Risque de liquidité
Le risque qu'un participant au système ne soit pas capable d'acquitter ses obligations financières au sein du système au moment prévu, mais il est en mesure de le faire ultérieurement.

3. Risque de défaillance de la banque de règlement
Risque que la banque de règlement (l'émetteur de l'actif qui sert au règlement) soit dans l'impossibilité de procéder au règlement. C'est principalement un risque de crédit ou de liquidité auquel la banque de règlement est exposée.

L'actif de règlement le plus sûr est la monnaie de banque centrale. Les participants au système détiennent une créance sur la banque centrale qui consiste en le solde de leurs comptes auprès de la banque centrale. C'est en général le cas pour les systèmes de règlement brut en temps réel[10].

Le règlement peut d'une manière similaire s'opérer par une banque commerciale. Auquel cas, l'actif de règlement est la monnaie commerciale.

4. Risque légal
Le risque que le cadre juridique inadéquat ou des incertitudes juridiques entraînent ou aggravent des risques de crédit ou de liquidité ou mettent en cause la finalité du règlement.

5. Risque opérationnel
Le risque que des défectuosités techniques ou des erreurs opérationnelles entraînent ou aggravent des risques de crédit ou de liquidité.

[10] RTGS -*Real time gross settlement system*

6. Risque d'inefficacité
Risque que les services du système soient trop coûteux en termes de ressources. L'inefficacité se traduirait par une augmentation de prix ou une baisse conséquente de performance ou de qualité.

Chaque catégorie de systèmes de paiement existant en nombre très limité par pays, il est très difficile de comparer l'efficience d'un système. Une comparaison internationale est possible. Elle sera toutefois biaisée par des conditions d'opération qui diffèrent.

2.1.4.2 Le risque systémique

Un système insuffisamment ou mal protégé contre les risques repris ci-dessus peut constituer un risque de défaillance pour lui-même et représenter un risque systémique. La défaillance du système ou de l'un de ses participants pourrait empêcher d'autres participants de respecter leurs obligations au sein du système, provoquant ainsi une instabilité globale du système.

La définition du risque systémique est plus complète lorsqu'elle englobe les conséquences plus étendues d'une défaillance. On tient compte dans ce cas du risque de propagation d'une défaillance à d'autres parties du secteur financier. Des institutions ne participant pas au système défaillant ne seraient plus en mesure de respecter leurs obligations à cause du système défaillant. La stabilité du secteur financier dans son ensemble serait menacée.

La définition du risque systémique prend toute son ampleur lorsqu'elle incorpore le risque de transmission d'une défaillance à d'autres sphères économiques. D'autres acteurs économiques ne seraient plus capables de respecter leurs obligations financières. La stabilité du système économique serait ébranlée.

On peut donc conclure que la robustesse d'un système de paiement revêt une importance particulière pour la stabilité financière et économique. C'est dans cette optique que les dix *Principes fondamentaux pour les systèmes de paiement d'importance systémique*[11] ont été adoptés en 2001 par la BRI. En raison de leur responsabilité de la stabilité financière, les banques centrales ont un rôle essentiel à jouer dans l'application de ces principes fondamentaux[12]. C'est ainsi que la surveillance prudentielle des systèmes de paiement et de règlement des opérations sur titres incombe généralement aux banques centrales. Dans certains pays, cette mission fait partie intégrante des statuts de la banque centrale (Australie, Canada, Irlande). Dans d'autres, elle ne repose pas sur un cadre juridique, elle fait l'objet d'un *memorandum of understanding* entre les parties responsables (Royaume-Uni, Danemark).

Le risque systémique est généralement associé aux systèmes de paiement de gros montants. Néanmoins, les systèmes de paiement de masse d'une certaine importance contribuent de manière significative à l'efficience et à la stabilité du secteur financier[13]. La catégorisation en tant que "système de paiement d'importance systémique" dépend de la situation du marché local. Elle est laissée au jugement des banques centrales. De la même manière, la distinction

[11] BRI - BIS, Comité sur les systèmes de paiement et de règlement, Principes fondamentaux pour les systèmes de paiement d'importance systémique, janvier 2001
SIPS -*Systemically Important Payment System*
[12] La BCE a également opté pour leur application aux SIPS.
[13] BRI - BIS, Committee on Payment and Settlement Systems, Policy issues for central banks in retail payments, September 2002

entre un système de paiement de gros montants et un système de paiement de masse est variable[14].

A l'origine, les principes fondamentaux ont été adoptés pour les SIPS. Toutefois, les systèmes de paiement de masse pourraient aussi recourir à cette approche.

L'applicabilité partielle et moins stricte des principes fondamentaux aux systèmes de paiement de masse a été examinée par l'Eurosystème pour les systèmes de paiement de masse dont la défaillance aurait des conséquences économiques graves et/ou un impact négatif sur la confiance en le système et en la monnaie. Il en résulte les "Normes de surveillances des systèmes de paiement de masse en euros" qui ont été adoptées par le Conseil des gouverneurs de la BCE le 26 juin 2003 dans le prolongement de la consultation publique du document lancée le 8 juillet 2002.

Les systèmes de paiement de masse ne sauraient être sous-estimés par une ampleur plus limitée du risque systémique. La perte de confiance et les perturbations engendrées par une défaillance remettraient en question la crédibilité du système et les instruments qui y sont associés, surtout s'ils sont nouveaux. Le dommage serait alors plus grave que la perte financière.

2.1.5 Effet de réseau

Les services de paiement (instruments et systèmes) ont les caractéristiques d'un bien de réseau, comme la téléphonie ou les chemins de fer par exemple. Chaque utilisateur profite de l'extension du réseau. En effet l'utilité qu'il en tirera sera d'autant plus importante que le nombre de ses participants augmente. Le fournisseur du service bénéficie aussi de l'extension de son réseau car les économies d'échelle feront baisser son coût unitaire et réduiront la probabilité d'émergence d'un réseau concurrent. Ceci peut conduire à deux craintes: la revendication d'un monopole naturel de la part des prestataires et le refus d'inter-connectivité du fournisseur initial, c'est-à-dire d'autoriser l'accès de son réseau à la concurrence. Ces questions d'interopérabilité et de concurrence sont prises en compte par les autorités de régulation et de concurrence, comme on le verra dans les chapitres consacrés au rôle des autorités et des banques centrales.

2.2 Cadre légal et réglementaire

Les systèmes et les instruments de paiement doivent tenir compte de plusieurs types de risques, dont le risque légal. Leur structure, leurs règles et conditions des opérations doivent être cohérentes et soutenues par un cadre légal et réglementaire. Ainsi, chacune des parties connaît ses responsabilités pour pouvoir les assumer.

Etant donné que le Grand-Duché de Luxembourg participe à la troisième phase de l'Union économique et monétaire, la Banque centrale du Luxembourg (BCL) fait partie intégrante du Système européen des banques centrales (SEBC). Le cadre juridique luxembourgeois dans les matières monétaires doit suivre la réglementation européenne et les orientations du SEBC.

[14] Ibid.

2.2.1 La législation luxembourgeoise

2.2.1.1 Législation concernant le secteur bancaire

Au Grand-Duché de Luxembourg, la loi du 5 avril 1993 est le cadre juridique principal relatif au secteur financier. Suivant la réglementation européenne, elle a subi des modifications pour prendre en compte les nouveaux instruments de paiement, tels que la monnaie électronique, et la protection des consommateurs lors de transactions électroniques.

Les systèmes de paiement ont une importance reconnue en matière de paiements. Il est primordial qu'ils assurent un règlement définitif.

- Loi du 5 avril 1993 relative au secteur financier

Un établissement de crédit, ou une banque, est défini comme une personne juridique "dont l'activité consiste à recevoir du public des dépôts ou d'autres fonds remboursables et à octroyer des crédits pour son propre compte." Cette activité nécessite un agrément ministériel et est soumise à la surveillance de la Commission de surveillance du secteur financier (CSSF).

Les systèmes de paiement ou de règlement des opérations sur titres sont repris dans la liste des professionnels du secteur financier (PSF) pour lesquels un agrément est également requis. Toutefois, ils sont considérés comme agréés de plein droit à partir du moment de leur notification à la Commission européenne par la BCL, justifiée par la participation de la BCL ou de toute autre entité du SEBC au système en question.

L'émission et la gestion de moyens de paiement (cartes de crédit, chèques de voyage, lettres de crédit) fait partie des activités autorisées aux établissements financiers d'origine communautaire. Celles-ci sont soumises à un contrôle par la CSSF.[15]

D'une manière générale, sont soumis au secret professionnel les entités suivantes: les administrateurs, membres des organes directeurs et de surveillance, dirigeants, employés et autres personnes qui sont au service des établissements de crédit, les autres professionnels du secteur financier, les organes de règlement, les contreparties centrales, les chambres de compensation et les opérateurs étrangers de systèmes agréés au Luxembourg.

La loi du 14 mai 2002 modifie cette loi du 5 avril 1993 en ce qui concerne les dispositions spécifiques aux émetteurs de monnaie électronique (directives 2000/28/CE et 2000/46/CE).

Une autre modification est intervenue avec la loi du 2 août 2003 qui soumet tout le secteur financier à la surveillance de la CSSF et qui crée de nouvelles catégories de PSF, notamment les opérateurs de systèmes informatiques et de réseaux de communication du secteur financier, également soumises à la surveillance prudentielle.

[15] La loi française du 24 janvier 1984, dite "loi bancaire" qui définit juridiquement les moyens de paiement, et réserve aux seuls établissements de crédit la "mise à disposition et la gestion des moyens de paiement" comme opération de banque à part entière, à côté des traditionnelles activités de réception de fonds du public et d'octroi de crédit.

- Loi du 14 mai 2002, concernant l'accès à l'activité des établissements de monnaie électronique, modifiant la loi du 5 avril 1993 et transposant les directives 2000/28/CE et 2000/46/CE

Cette loi institue les "établissements de monnaie électronique" ou ELMI[16] dont l'activité principale est d'émettre des moyens de paiement sous forme de monnaie électronique en échange de fonds. Ils ne sont pas autorisés à octroyer du crédit ni à recevoir de dépôts. Les fonds reçus sont immédiatement convertis en monnaie électronique.

La monnaie électronique est définie comme un droit de créance d'une valeur non inférieure à la valeur des fonds remis en échange, stocké sur un support électronique et accepté comme moyen de paiement par d'autres parties que l'émetteur. La monnaie électronique peut aussi être émise par un établissement de crédit.

Les activités autorisées aux ELMI sont limitées. Ils sont néanmoins assujettis à une obligation de réserves obligatoires[17].

Les conditions de remboursabilité de la monnaie électronique sont plus strictes que la directive 2000/46/CE. La loi luxembourgeoise exige que le détenteur puisse en exiger le remboursement "en cas de perte, vol, destruction ou défaut technique du support de la monnaie électronique, sous réserve que la valeur de la monnaie électronique soit techniquement déterminable."

L'activité d'émission de monnaie électronique est soumise à la même procédure d'agrément que les établissements de crédit. Toutefois, les ELMI peuvent demander une exemption quant à l'application de certaines dispositions: lorsque le montant total des engagements liés à la monnaie électronique en circulation ne dépasse normalement pas 5 millions d'euros (et à aucun moment 6 millions d'euros), lorsque la monnaie électronique émise n'est acceptée que par des filiales de l'émetteur ou dans une zone géographique restreinte.

La loi indique que la capacité maximale des supports de monnaie électronique ne peut pas dépasser 150 euros.

- Loi du 12 janvier 2001, transposant la directive 98/26/CE dans la loi du 5 avril 1993, relative au caractère définitif du règlement dans les systèmes de paiement

Cette loi définit les conditions d'agrément et de surveillance prudentielle des systèmes de paiement et des systèmes de règlement des opérations sur titres. Les conséquences de la notification d'un système à la Commission européenne ont été vues ci-dessus. La surveillance de tels systèmes relève alors de la seule compétence de la BCL.

Les systèmes de paiement notifiés par le Grand-Duché de Luxembourg sont LIPS-Gross et LIPS-Net[18] auxquels la BCL participe.

---

[16] *EL*ectronic *M*oney *I*nstitution

[17] Règlement No 690/2002 de la Banque centrale européenne du 18 avril 2002 modifiant le règlement no 2818/98 (BCE/1998/15) concernant l'application de réserves obligatoires

[18] LIPS-Gross - *Luxembourg Interbank Payment System- Real Time Gross Settlement System-* est le système de règlement brut en temps réel en place au Grand-Duché de Luxembourg.
LIPS-Net - *Luxembourg Interbank Payment System- Netting System-* est le système de compensation électronique au Grand-Duché de Luxembourg.

L'absence de participation de la BCL dans un système n'exclut pas totalement sa compétence en la matière. La mission de surveillance est partagée avec la CSSF, par exemple en ce qui concerne les systèmes de transferts de monnaie électronique et les systèmes de transferts électroniques liés à l'utilisation de cartes bancaires.

La mission de surveillance elle-même n'est pas organisée par la loi.

- Loi du 23 décembre 1998, relative au statut monétaire et à la Banque centrale du Luxembourg

"Le statut monétaire du Grand-Duché de Luxembourg est celui d'un Etat membre de la Communauté européenne qui a adopté la monnaie unique, l'euro."

Les signes monétaires (billets et pièces) libellés en euro ont donc cours légal dans la Communauté européenne et force libératoire, en vertu des règles communautaires applicables.

Il est à noter que la loi n'attribue pas de fonctions consultatives à la BCL, ni de pouvoir réglementaire. La BCL doit remplir les missions générales qui lui sont attribuées au niveau national et au niveau communautaire.

2.2.1.2 Législation favorisant le commerce électronique

Le commerce dit électronique et l'accès électronique aux services bancaires trouvent une base légale grâce notamment à la loi relative au commerce électronique et au traitement égalitaire de la signature électronique par rapport à la signature manuscrite.

- Loi du 14 août 2000, relative au commerce électronique et transposant les directives 1999/93 et 2000/31/CE et certaines dispositions de la directive 97/7CEE

Cette loi vise particulièrement la sécurisation du commerce électronique. Elle couvre notamment les domaines suivants: les effets juridiques de la signature électronique, la conclusion de contrats par voie électronique et les paiements électroniques.

La signature est manuscrite ou électronique, sans que l'on puisse être contraint à utiliser cette dernière. La signature identifie le signataire et exprime l'assentiment de ce dernier quant à l'acte qu'il signe. Lorsqu'elle est digitale, la signature consiste en données électroniques indissociables de l'acte dont elle certifie l'intégrité.

La signature électronique ne pourra être refusée par un juge comme moyen de preuve et sera assimilée à la signature manuscrite lorsqu'elle repose sur un certificat qualifié, dont le contrôle d'émission est plus rigoureux. La reconnaissance des effets juridiques de la signature électronique ouvre la possibilité de conclure des contrats électroniques et des paiements électroniques.

Les prestataires de service de certification délivrant des certificats qualifiés peuvent souscrire à un régime volontaire d'accréditation, gage de qualité. Au Grand-Duché de Luxembourg, c'est à l'Office Luxembourgeois d'Accréditation et de Surveillance (OLAS), l'autorité nationale d'accréditation et de surveillance, qu'incombe cette fonction.

La conclusion de contrats par un moyen électronique est reconnue entre professionnels et entre professionnels et consommateurs. Sont définis dans le texte de loi les étapes de la conclusion dudit contrat, sa date de conclusion et de livraison, le droit de rétraction du consommateur, les informations à fournir, les conditions de paiement…

Ce texte de loi se base sur la recommandation 97/489/CE en ce qui concerne l'information des consommateurs pour les paiements électroniques. Il ne fait toutefois pas mention explicitement de la recommandation et ne la transcrit pas complètement. Sont exclus de la loi, les chèques et la monnaie électronique détachée de tout compte de chargement et de déchargement et qui n'est utilisable qu'auprès d'un vendeur. L'émetteur de l'instrument de paiement doit conserver un relevé interne des opérations pendant les trois années (une "période suffisamment longue" selon la recommandation) suivant l'exécution des opérations. En cas de contestation, il doit pouvoir prouver que l'opération a été comptabilisée correctement et qu'aucune défaillance (technique ou autre) ne l'ait affectée. La responsabilité du titulaire, non frauduleux ni gravement négligent, est limitée à 150 euros jusqu'au moment où il notifie le vol ou la perte. L'utilisation d'un instrument sans sa présentation physique ou sans identification électronique dégage la responsabilité de son titulaire. Sauf s'il ne connaît pas le montant de l'instruction de paiement, le détenteur ne peut révoquer une instruction de paiement donnée au moyen de son instrument électronique.

- Règlement grand-ducal du 1er juin 2001, relatif aux signatures électroniques, au paiement électronique et à la création du "comité commerce électronique"

Ce règlement précise, entre autres, les définitions du "certificat qualifié" et de la "signature électronique du prestataire de services de certification délivrant des certificats qualifiés". Il détermine aussi les exigences relatives au certificat qualifié, aux prestataires de service de certification délivrant des certificats (qualifiés) et aux dispositifs sécurisés de création de signature électronique.

2.2.2 La législation européenne

La norme législative communautaire prime sur la norme législative nationale de niveau équivalent. C'est ainsi que les textes mentionnés dans le chapitre précédent tiennent compte de la norme européenne contraignante.

2.2.2.1 Législation concernant le secteur bancaire et les paiements

Il est intéressant de noter que la législation actuelle couvre l'activité des établissements de crédit, la finalité du règlement des systèmes de paiement et de règlement des opérations sur titres, la monnaie électronique, le commerce électronique et la signature digitale. Aucune législation contraignante n'adresse spécifiquement les paiements électroniques.

- Recommandation 97/489/CE de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire

La recommandation s'applique aux transferts de fonds et aux retraits d'argent liquide effectués au moyen d'un instrument de paiement électronique (carte de paiement, porte-monnaie électronique, banque à distance) ainsi qu'au chargement et au déchargement d'un instrument de monnaie électronique.

Le but de cette recommandation est d'accroître la transparence contractuelle entre les émetteurs d'instruments de paiement électroniques et leurs titulaires. Les conditions relatives à l'usage d'un instrument de paiement électronique (coût, description, taux d'intérêt, frais et commissions en cas d'utilisation à l'étranger…) et les obligations et responsabilités des parties (précautions élémentaires, relevé des opérations…) devront être présentées par écrit en "termes simples et aisément compréhensibles".

La responsabilité du titulaire est engagée à hauteur de 150 euros maximum en cas de perte ou de vol, sauf en cas de négligence extrême ou de fraude. Ce montant de responsabilité financière, ainsi que d'autres éléments de la recommandation, sont repris dans la loi du 14 août 2000.

- Directive 2000/12/CE du Parlement européen et du Conseil du 20 mars 2000 concernant l'accès à l'activité des établissements de crédit et son exercice

L'objectif de cette directive est la réalisation du marché intérieur dans le secteur des établissements de crédit, par la liberté d'établissement et la libre prestation de services.

La directive est appliquée par les modifications apportées à la loi du 5 avril 1993 relative au secteur financier.

Les articles de la directive 2000/12/CE correspondent directement à des articles des directives 77/780/CEE, 89/299/CEE, 89/646/CEE, 89/647/CEE, 92/30/CEE, 92/121/CEE et 96/10/CE.

- Directive 2000/28/CE du Parlement européen et du Conseil du 18 septembre 2000 modifiant la directive 2000/12/CE concernant l'accès à l'activité des établissements de crédit et son exercice

Cette directive incorpore explicitement la définition d'"établissement de monnaie électronique" dans celle d'"établissement de crédit".

- Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements

Cette directive introduit la définition de la "monnaie électronique" et des "établissements de monnaie électronique".

Dans l'ensemble, les références aux établissements de crédit de la directive concernant l'accès à l'activité d'établissement de crédit (2000/12/CE) s'appliquent aux établissements de monnaie électronique. Mais les activités et les placements autorisés à ces derniers sont limités.

Il est important de noter que les ELMI ne sont pas couvertes par la directive touchant au caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres.

Comme repris dans la loi luxembourgeoise du 14 mai 2002, une exemption aux dispositions de la présente directive et de la directive 2000/12/CE peut être accordée dans certaines conditions. Les établissements de monnaie électronique bénéficiant d'une exemption ne peuvent toutefois pas prétendre à la reconnaissance mutuelle indiquée dans la directive 2000/12/CE.
Par cette directive, le législateur européen donne la possibilité à des non-banques de se positionner sur le marché des transactions de paiement numéraire.

- Directive 98/26/CE du Parlement européen et du Conseil du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres, la SFD *-Settlement Finality Directive-*

Il est essentiel de réduire l'incertitude associée à la participation à un système de paiement, que celui-ci fonctionne sur base d'une compensation multilatérale ou d'un règlement brut en temps réel. La réduction du risque systémique requiert le caractère définitif du règlement et le recouvrement des garanties. Les ordres de transfert et leur compensation doivent donc produire leurs effets en droit dans tous les Etats membres et être opposables aux tiers lorsqu'ils sont rentrés dans le système avant l'ouverture de toute procédure d'insolvabilité à l'encontre d'un participant. En outre, les ordres de transfert ne peuvent pas être révoqués.

Afin d'être couvert par le caractère définitif du règlement, un système doit être notifié à la Commission européenne.

La directive est appliquée par la loi du 12 janvier 2001, transposant la directive 98/26/CE dans la loi du 5 avril 1993, relative au caractère définitif du règlement dans les systèmes de paiement.

2.2.2.2 Législation favorisant le commerce électronique

- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques

L'objectif de cette directive est de faciliter l'usage des signatures électroniques et de leur attribuer une reconnaissance juridique dans tous les Etats membres. La reconnaissance de certificats qualifiés émis dans des Etats tiers comme équivalents à des certificats qualifiés émis dans un Etat membre est possible sous certaines conditions.

La fourniture de services de certification nécessaires aux signatures électroniques n'est soumise à aucune autorisation préalable. Néanmoins, les Etats membres doivent donner à ces prestataires de service la possibilité d'une accréditation volontaire, synonyme de qualité de service.

La signature digitale est un apport important pour le commerce et les paiements électroniques. Il rend le consommateur légalement responsable de son ordre d'achat, même transfrontalier. La

signature électronique permet aussi à des intervenants non bancaires (tels que des opérateurs de téléphonie) d'offrir des services de paiement.

Cette directive a été transposée dans le Règlement grand-ducal du 1er juin 2001, relatif aux signatures électroniques, au paiement électronique et à la création du "comité commerce électronique" et dans la loi du 14 août 2000, relative au commerce électronique et transposant la directive 1999/93 et certaines dispositions de la directive 97/7CEE.

- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 ou "directive sur le commerce électronique"

Pour le développement des services de la société de l'information, il faut garantir la sécurité juridique et inciter les consommateurs à la confiance. Dans cette optique, la présente directive veut créer un cadre juridique pour assurer la libre circulation des services de la société de l'information entre les Etats membres.

Ainsi, cette directive rend possible la conclusion de contrats par voie électronique (exception faite de l'immobilier, du droit de la famille…) entre prestataires de services et entre prestataires de services et consommateurs.

La directive touche par ailleurs à l'accès à l'activité de prestataire de services, aux communications commerciales (sollicitées ou non) et à la responsabilité des prestataires intermédiaires.

Cette directive a été transposée dans la loi du 14 août 2000.

- Directive 2001/115/CE du Conseil du 20 décembre 2001 modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée

Cette directive uniformise les règles de facturation applicables à l'ensemble des Etats membres. D'autre part, elle autorise les entreprises à recourir à la facturation électronique. Toutefois, son acceptation ne saurait être forcée.

La signature digitale est requise pour garantir l'authenticité de la facture.

Cette directive est à transposer au plus tard le 1er janvier 2004. C'est chose faite avec la loi du 1er juillet 2003 modifiant et complétant la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée. D'autre part, cette loi applique la directive 2002/38/CE du Conseil du 7 mai 2002 modifiant, en partie à titre temporaire, la directive 77/388/CEE en ce qui concerne le régime de taxe sur la valeur ajoutée applicable aux services de radiodiffusion et de télévision et à certains services fournis par voie électronique.

- Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE

L'objet de cette directive est de rapprocher les dispositions relatives à la commercialisation à distance de services financiers auprès des consommateurs. Son application doit être conforme à la directive 2000/31/CE sur le commerce électronique qui s'applique aux transactions qu'elle couvre.

La définition de "services financiers" comprend notamment tout service relatif à la banque et aux paiements.

Un ensemble d'informations au consommateur est obligatoire avant la conclusion du contrat à distance. Le consommateur peut se rétracter dans un délai 14 jours (porté à 30 jours pour certains contrats). Le droit de rétraction ne s'applique pas à tous les services.

Le consommateur doit avoir la possibilité de demander l'annulation d'un paiement en cas d'utilisation frauduleuse de sa carte de paiement pour la conclusion d'un contrat à distance.

La directive est à transposer au plus tard le 9 octobre 2004. Certaines de ses dispositions sont déjà présentes dans la loi luxembourgeoise du 14 août 2000 sur le commerce électronique. La loi reprend en effet certaines dispositions de la directive 97/7/CE (concernant la protection des consommateurs en matière de contrats à distance) qui elle-même se trouve modifiée par la présente directive.

2.2.3 Rôle des autorités et des banques centrales

Il est de la responsabilité générale des autorités publiques, et des autorités monétaires en particulier, de promouvoir et de maintenir la sécurité et l'efficience des systèmes et des instruments de paiement. Ceux-ci jouent en effet un rôle prépondérant dans la transmission de la politique monétaire, dans les échanges économiques et dans la stabilité financière. Les banques centrales sont d'autre part considérées comme des intervenants neutres ayant un intérêt particulier dans la stabilité financière. Dès lors, une intervention des autorités publiques et des banques centrales dans la fourniture de services de paiement est justifiée, non seulement pour les systèmes de gros montants mais aussi pour les paiements de masse.

Par ses fonctions de banquier des banques centrales et d'organisation visant à favoriser la coopération monétaire et financière internationale, les travaux et conclusions de la Banque des Règlements Internationaux (BRI) et plus particulièrement de son Comité sur les systèmes de paiement et de règlement (CSPR) -*Committee on Payment and Settlement Systems (CPSS)*- en matière de politique des systèmes et des instruments de paiement sont pris en compte par les autorités nationales et les banques centrales dont le SEBC.

Le rapport *Policy issues for central banks in retail payments* du CSPR, dont la consultation publique s'est terminée le 13 décembre 2002, fait état de la contribution significative des systèmes et des instruments de paiement de masse à l'efficience et à la stabilité du système financier. Le rapport s'interroge sur les conséquences de l'évolution des paiements de masse (innovations technologiques, paiements transfrontaliers, nouveaux intervenants, nouveaux canaux tels que Internet et les appareils mobiles...) sur leur efficacité et sur leur sécurité. Ces conséquences sont prises en considération dans les quatre domaines de politique des banques centrales et les objectifs qui leur sont liés:

1. Cadre légal et réglementaire: s'attaquer aux barrières aux innovations et au développement du marché;
2. Structure et performance de marché: favoriser les conditions de concurrence de marché;
3. Standards et infrastructure: soutenir le développement de standards et d'infrastructures efficaces;
4. Services de banque centrale: fournir les services aussi efficacement que possible pour le marché défini.

Les objectifs de politique publique en matière de paiements de masse sont principalement d'assurer leur sécurité et leur efficience.

Un niveau de sécurité très rigoureux implique des investissements et des coûts d'exploitation élevés, ainsi que des procédures fastidieuses, souvent au détriment de l'efficience du système. Dès lors, un compromis entre sécurité et efficience s'avère nécessaire afin de ne pas diminuer l'utilité du système. Le principe fondamental VIII afférents aux SIPS admet cette nécessité de compromis[19]. Une argumentation similaire prévaut pour les paiements de masse. L'Eurosystème reprend ce principe d'efficience parmi les 6 principes qui seraient applicables aux systèmes de paiement de masse.

L'interopérabilité d'un système contribue à son efficience. Elle passe en général par l'établissement de normes techniques et sécuritaires. Néanmoins une normalisation trop poussée comporte deux risques principaux: inhiber les innovations et pousser à l'utilisation de systèmes propriétaires jugés plus sûrs sur base de leur technologie non divulguée.

Les actions que les banques centrales peuvent entreprendre dans le cadre de ces politiques sont:
1. L'observation des conditions du marché et de leur évolution;
2. Faire usage de leur rôle de catalyseur en participant à des groupes de travail et en conseillant les acteurs des secteurs public et privé;
3. Exploiter un système;
4. Procéder à l'oversight (surveillance) des systèmes.

La dernière phrase concluant le rapport *Policy issues for central banks in retail payments* identifie correctement la nécessaire évolution des banques centrales: "As the economy develops, the role of the central bank needs to be reviewed."

Ainsi, il conviendrait aux régulateurs de surveiller l'évolution des acteurs non-bancaires dans l'approvisionnement de services bancaires ou de paiement. Une supervision prudentielle pourrait même se justifier dans l'optique d'assurer l'intégrité financière et la protection des consommateurs, tout en prenant les précautions utiles pour ne pas entraver les innovations.

[19] Principe fondamental VIII: "Le système doit fournir un mode de paiement à la fois pratique pour ses utilisateurs et efficient pour l'économie.", BRI - BIS, Comité sur les systèmes de paiement et de règlement, Principes fondamentaux pour les systèmes de paiement d'importance systémique, janvier 2001

2.2.4 Rôle du Système européen des banques centrales

Le SEBC et la BCE sont érigés par le Traité instituant la Communauté européenne. Leurs compétences s'établissent dans le domaine de la politique monétaire.

En ce qui concerne les systèmes de paiement, la mission définie à l'article 105 (2) du Traité consiste pour le SEBC à promouvoir leur bon fonctionnement. La définition de cette mission fondamentale n'est pas très précise, aucune responsabilité ni aucun cadre opérationnel ne sont mis en avant. Le SEBC distingue donc lui-même sa responsabilité de s'intéresser au fonctionnement des systèmes de paiement et à leur sécurité, impliquant notamment un rôle de supervision.

Selon l'article 105.4 du Traité, la BCE est consultée sur les projets de réglementation nationale et d'acte communautaire dans les domaines relevant de sa compétence. La BCE bénéficie aussi d'un droit d'initiative dans ces domaines, par la soumission de son avis aux autorités nationales, institutions et organes communautaires.

Suivant l'article 110 du Traité, l'accomplissement des missions du SEBC autorise la BCE à:
- Arrêter des règlements, de portée générale et applicables directement dans tout Etat membre;
- Prendre des décisions, obligatoires dans tous ses éléments aux destinataires qu'elle désigne;
- Emettre des recommandations et des avis, qui n'ont pas de pouvoir contraignant.

Ces pouvoirs réglementaires sont aussi valables dans le cadre de la promotion du bon fonctionnement des systèmes de paiement si l'on se réfère à l'article 34.1 (il renvoie directement à l'article 110 du Traité) des Statuts du SEBC.

L'article 22[20] du Protocole sur les Statuts du SEBC précise que dans le domaine des systèmes de compensation et de paiement, la BCE et les banques centrales nationales peuvent fournir des facilités et que la BCE peut arrêter des règlements.

Les objectifs de la politique des systèmes de paiement du SEBC peuvent donc se résumer en 4 points:
1. Maintenir la stabilité systémique;
2. Assurer l'efficience des systèmes de paiement;
3. Maintenir la confiance du public dans les instruments de paiement et dans la monnaie;
4. Protéger le canal de transmission de la politique monétaire

Dans ce contexte, l'Eurosystème intervient jusqu'à présent de trois manières dans le domaine des systèmes de paiement:

[20] Article 22 - Systèmes de compensation et de paiements: La BCE et les banques centrales nationales peuvent accorder des facilités, et la BCE peut arrêter des règlements, en vue d'assurer l'efficacité et la solidité des systèmes de compensation et de paiements au sein de la Communauté et avec les pays tiers.

1. La fourniture de services: participation commune à TARGET[21] -*Trans-European Automated Real-time Gross Settlement Express Transfer system*- avec un degré d'implication dans les systèmes de paiement de masse en fonction des circonstances nationales;
2. L'oversight: établissement de standards communs de sécurité et d'efficience avec une application décentralisée;
3. La facilitation des initiatives du marché: dans un objectif d'établir des standards opérationnels et sécuritaires tant au niveau national que pour la zone euro.

Le point 1 ci-dessus résulte directement de l'application de la première partie de l'article 22 des Statuts. Le seconde partie de ce même article, l'adoption de règlements concernant les systèmes de paiement et de compensation, n'a pas encore été exercée par la BCE.

L'Eurosystème accorde un intérêt incontestable à l'efficience et à la sécurité des instruments et des systèmes de paiement nationaux et transfrontaliers. L'importance de ces derniers croît dans le cadre de la création d'une zone unique de paiement -*Single Payment Area*. L'Eurosystème conçoit son rôle dans la promotion de l'efficience et de la sécurité des systèmes. En témoignent ses consultations publiques sur les objectifs de sécurité de la monnaie électronique et sur l'application des principes fondamentaux aux systèmes de paiement de masse, ainsi que les discussions touchant au cadre légal du *Single Payment Area*[22]. L'Eurosystème et les banques centrales nationales peuvent faire valoir leur rôle de catalyseur du marché pour participer à l'établissement des objectifs et des normes de sécurité, favoriser l'interopérabilité des systèmes et des instruments et ainsi rendre les systèmes plus efficients et plus sûrs.

3 Les nouveaux instruments de paiement

La question des micro-paiements, les paiements de "petit montant", resurgit pour les paiements électroniques. Elle ne se posait pas pour la monnaie fiduciaire et avait été soulevée pour les paiements scripturaux. Des limites minimales de transaction sont parfois appliquées par les commerçants sur certains instruments.

Les micro-paiements sont souvent limités à 10 euros maximum. Pour certains, ils doivent être inférieurs à 5 euros; pour d'autres, inférieurs à 25 euros. Le but n'est pas de spéculer sur le montant d'un micro-paiement mais de mettre en évidence le montant de paiement pour lequel le traitement par les banques est assez coûteux (comparativement aux paiements de valeur plus élevée) et pour lequel un nouvel intervenant pourrait se révéler plus compétitif et plus efficient. On considérera dans la suite de ce document un micro-paiement de maximum 10 euros.

Cette distinction a aussi son importance du point de vue de la politique de sécurité. Celle-ci sera relativement moins stricte pour un paiement de petite valeur, avec par exemple un niveau d'authentification plus faible. Le coût et la complexité d'une signature électronique seraient alors disproportionnés par rapport au montant de la transaction.

[21] Système de paiement composé d'un système de règlement brut en temps réel dans chacun des États membres de l'UE et du mécanisme de paiement de la BCE.
[22] Le marché a aussi entrepris l'initiative d'un *White Paper on the single euro payments area (SEPA)*

Il est intéressant de noter que l'Eurosystème fait mention de "paiements électroniques de faible montant"[23] sans indiquer de limite supérieure. La directive 2000/46/CE concernant les ELMI indique que la capacité maximale de chargement d'un instrument de monnaie électronique est fixée à 150 euros. Le règlement 2560/2001 concernant les paiements transfrontaliers en euros effectués par les consommateurs et les petites et moyennes entreprises porte pour le moment sur les opérations transfrontalières de paiement électronique d'un montant maximum de 12500 euros.

3.1 Définitions

3.1.1 Paiements électroniques

L'évolution technologique et leur application au domaine des paiements modifient les mécanismes de paiement existants et permettent le déploiement de nouvelles solutions de paiement. La Banque centrale européenne (BCE) considère comme un paiement électronique, un *e-payment*[24], tout paiement initié et traité de manière électronique.

Lorsque l'on analyse un paiement de masse, un virement dans l'exemple de la figure 1, les parties manifestes pour les consommateurs sont l'émission de l'instruction de paiement et sa confirmation (point 2 pris en considération bilatéralement). Depuis quelques années, on note une tendance à la faveur des instruments de paiements électroniques[25] de masse. Les innovations touchant aux instruments de paiements portent principalement sur l'initiation de l'instruction de paiement mais aussi sur la confirmation du paiement en temps (quasi) réel.

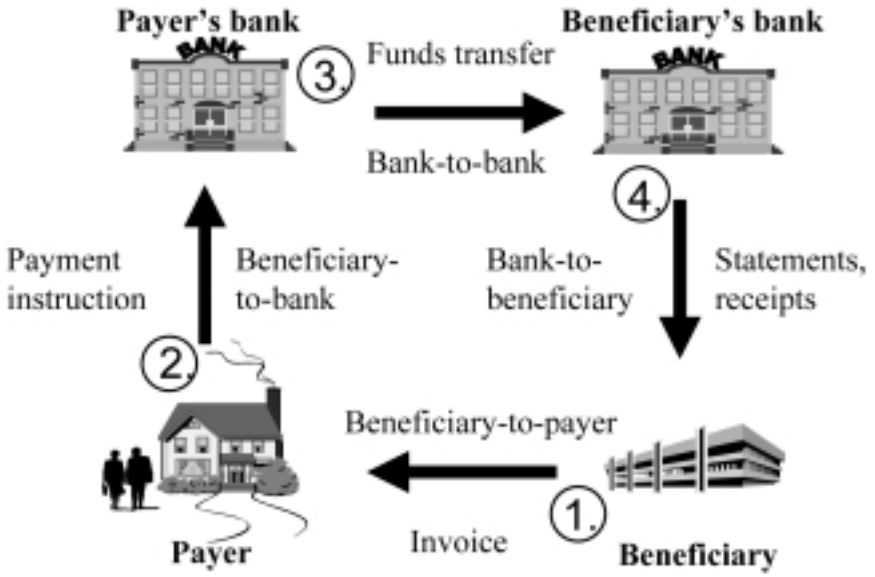
Le règlement interbancaire (point 3) est déjà majoritairement électronique en Europe et s'effectue par les systèmes de paiement dont il a été question dans le paragraphe Les systèmes de paiement.

La réconciliation des paiements (point 4) est déjà possible de manière électronique pour les grandes sociétés.

La facturation électronique (point 1) ne fait pas partie de l'action de payer, au sens du transfert de la créance monétaire. Il en sera fait mention dans le paragraphe consacré à l'Automatisation de bout en bout.

[23] BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002
[24] BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002
[25] BRI - BIS, Committee on Payment and Settlement Systems, Retail Payments in Selected Countries: A Comparative Study, September 1999

Figure 1: Cycle de paiement par virement [26]



Beaucoup de solutions de paiement électronique ont vu le jour: l'ePSO[27] -*Electronic Payment Systems Observatory*- en a dénombré près de 180 en novembre 2001 en Europe. Mais aucune d'entre elles n'a réellement émergé. Très certainement, le cantonnement national, les limitations commerciales et techniques des solutions ainsi que le manque d'interopérabilité ne favorisent pas une adoption en masse.

Parmi les instruments de paiement électroniques, la BCE[28] distingue les instruments existants qui ont été adaptés à un usage sur Internet des nouveaux instruments de paiement.

Exemples d'instruments adaptés à Internet

- Cartes de crédit
  Prenant avantage d'un réseau international qui a fait ses preuves, c'est l'instrument le plus utilisé pour les achats par Internet malgré certains problèmes de sécurité (fraude).

- Virements
  Les virements sont déjà très répandus. Ils commencent à être utilisés comme instrument de paiement pour le *e-commerce* mais ils sont généralement limités à des transactions nationales.

- Domiciliations et cartes de débit
  Le bénéficiaire a l'autorisation de débiter directement le montant du compte du client. Cet instrument de paiement est relativement peu utilisé pour le commerce par Internet. Il est peu approprié pour les transactions transfrontalières.

[26] BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002, adapté de H. Leinonen, Bank of Finland, Discussion paper 17
[27] Carat Gérard, Background Paper No. 9, March 2002
[28] BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002

Exemples de nouvelles solutions de paiement

- Monnaie électronique (sur carte à puce ou sur réseau) et cartes prépayées
  Le client transfère par avance sur le support un montant pour l'échanger en monnaie électronique. Son acceptation est faible, probablement à cause d'une interopérabilité insuffisante et de coûts élevés pour les commerçants.

  Exemples: Proton (Belgique), miniCASH (Luxembourg).

- Paiements en ligne de particulier à particulier
  Un compte lié à une adresse e-mail et propriétaire à ce système sert à effectuer des paiements par virement entre les membres. Fonctionnant sur une base prépayée, ce compte est crédité au moyen d'instruments "traditionnels": virement, carte de crédit, chèque, etc. Son solde est disponible pour d'autres virements ou pour une restitution sur un compte bancaire.

  Exemple: PayPal (Etats-Unis).

- Portails de paiement
  Portail spécialisé dont le but est de servir de point unique de services de paiement aux vendeurs à distance (Internet, catalogues, etc.) en offrant plusieurs solutions de paiement aux acheteurs: chèque, virement manuel et électronique, carte de crédit, débit direct.

  Exemples: Bibit (Allemagne), Etrasfot (Belgique).

- Paiements par téléphone mobile.
  Le téléphone mobile sert à identifier le client et à communiquer le paiement au prestataire de service. Ce type de solution est détaillé dans Les paiements mobiles.

Hormis la monnaie électronique, les nouvelles solutions de paiement signalées ici reposent en définitive sur des instruments de paiement scripturaux existants: cartes de crédit, virements, cartes de débit... La distinction faite pour les "nouveaux" instruments de paiement se fonde sur l'utilisation de technologies nouvellement appliquées aux paiements. Ce sont des paiements électroniques qui utilisent la monnaie scripturale. On leur reconnaît donc les mêmes caractéristiques que pour les instruments de paiements scripturaux existants, voir le paragraphe concernant Les instruments de paiement. Principalement, ces instruments ne sont pas dotés du cours légal et le règlement requiert toujours une intervention bancaire.

3.1.2 La monnaie électronique

Parmi les instruments de paiement électroniques, la monnaie électronique pourrait constituer une exception et jouir du cours légal dans le cadre d'une émission par une banque centrale ou d'une émission certifiée par celle-ci. La République de Singapour vise à devenir le premier Etat à établir un système de monnaie légale électronique pour 2008. Dans le *Singapore Electronic*

Legal Tender System (SELT), la monnaie serait émise par le *Board of Commissioners of Currency* qui est l'autorité légalement responsable de l'émission de la monnaie. Le SEBC s'est réservé cette possibilité d'émettre de la monnaie électronique[29].

La monnaie électronique émise par un établissement autre que la banque centrale diffère de la monnaie fiduciaire car elle ne constitue pas une créance à l'encontre de l'Etat. Lors d'un retrait de billets de banque par débit de son compte bancaire, le passif et l'actif de la banque diminuent. Lors du rechargement d'un porte-monnaie électronique (toujours par le débit du compte bancaire), il y a transfert entre comptes de passif de la banque.

La transmissibilité est une autre différence majeure entre ces deux sortes de monnaie. En raison de risques élevés de fraude et d'exigences légales de remboursabilité, même en cas de perte du support de la monnaie, les systèmes déployés fonctionnent sur base d'un remboursement par l'émetteur après chaque transaction, rendant la transmissibilité impossible. Ils sont qualifiés de système de circulation fermé et permettent d'identifier le détenteur.

Dans un système de circulation ouvert, la monnaie électronique circulant librement (sans contrôle de l'émetteur à chaque transaction) a les mêmes caractéristiques de transmissibilité et d'anonymat que les billets de banque.

Au niveau de l'émetteur de la monnaie, le compte de "monnaie électronique émise" s'apparente à un dépôt à court terme. Il pourrait, comme tout dépôt, même être rémunéré.

3.1.3 Les paiements mobiles

3.1.3.1 Identification

La BCE désigne sous l'appellation de paiement mobile, un *m-payment*[30], l'utilisation d'un téléphone mobile (via un SMS -*Short Message Service*- ou un appel téléphonique) pour l'émission d'un paiement. Les paiements mobiles étant émis et traités électroniquement, ils font partie intégrante des paiements électroniques.

Le cantonnement de cette définition aux téléphones mobiles pourrait s'avérer trop restrictif face aux développements d'autres technologies. Le téléphone mobile n'est pas le seul équipement permettant l'accès aux réseaux de communication sans fil. Les PDA -*Personal Digital Assistant*- et ordinateurs sont autant de possibilités. En outre, plusieurs réseaux sans fil, dont certains ne fournissent pas de service de voix, coexistent par l'application de standards différents[31] qui sont à prendre en compte pour le développement des normes des paiements mobiles.

Cette définition de "paiement mobile" est elle-même assez exhaustive. L'utilisation du téléphone mobile ne saurait être limitée à l'émission d'un paiement. Son intervention dans le

[29] "The ECB will continue to monitor developments in the field of electronic money and to reassess its effects on monetary policy and the integrity of payment systems, and may have to define new policy conclusions, including, if necessary, the issuance of electronic money by the ESCB itself", BCE - ECB, Report on Electronic Money, August 1998

[30] "Several initiatives have emerged for initiating e-payments from mobile phones by using short messages (SMS) or phone calls.", BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002

[31] Voir Annexe 2

cadre des paiements est variée, comme nous le verrons dans le chapitre détaillant quelques exemples. En outre, le terminal mobile peut servir de point d'accès au compte bancaire et aux services bancaires (y compris les paiements); c'est le *m-banking*.

3.1.3.2 Pertinence des paiements mobiles

Partant du constat de sa très bonne intégration[32], de ses capacités de calcul et de ses possibilités techniques, le téléphone mobile apparaît potentiellement comme un très bon outil pour les paiements de masse. Il a en outre l'avantage d'être ubiquitaire au niveau national et international et de pouvoir relier des personnes entre elles. Ce qui permet d'effectuer un paiement à partir de n'importe quelle localisation et en faveur d'une autre personne.

Des solutions de paiement mobile sont mises en service depuis quelques années, principalement en Europe. Leur succès limité laisse à penser que ces offres sont plutôt poussées par les banques, les opérateurs et les constructeurs que demandées par les utilisateurs. Néanmoins, l'efficience présumée des paiements mobiles incite autant les autorités que les entreprises privées à s'y intéresser, et éventuellement à promouvoir leur adoption.

3.1.3.2.1 Demande des utilisateurs

De par son adoption très rapide, le téléphone mobile serait en passe de devenir un bien de commodité et l'appareil préféré des consommateurs. Au Grand-Duché de Luxembourg, 4 ménages sur 5 possèdent un téléphone mobile[33]. Ce dernier sert aux communications verbales et écrites, et éventuellement à surfer sur des pages Internet au format ajusté. Les fonctionnalités du téléphone mobile non liées à la téléphonie (agenda, carnet d'adresse, réveil, SMS, etc.) dont font usage les utilisateurs laissent entrevoir une propension à s'en servir également pour les paiements. Ici, la simplicité d'utilisation est importante pour une acceptation à grande échelle. La taille limitée de l'écran d'un téléphone mobile ne permet pas la visualisation de toute l'information en un seul affichage, le défilement de menus et d'écrans peut par exemple être perturbant.

Une demande certaine pour les paiements par mobile existe. Une étude menée en collaboration avec le Judge Institute of Management, Cambridge University[34] indique que 44% des personnes interrogées seraient enclines à faire usage de leur téléphone mobile pour les micro-paiements via un système de *m-money* (monnaie mobile). Une autre étude de e-Mori[35] confirme que sur les 6 pays inventoriés, environ 50% des personnes utiliseraient leur téléphone mobile en remplacement de la monnaie (distributeurs automatiques, tickets…) et pour payer des factures. 20 à 50% des personnes seraient prêtes à faire intervenir le téléphone mobile pour des achats en ligne.

Le terminal mobile demeure en quasi permanence avec son propriétaire. C'est un avantage sécurisant car ce dernier serait immédiatement avisé de sa disparition; l'intrusion dans un ordinateur ou sa disparition n'est observée que plusieurs heures, voire jours, plus tard. Le terminal qui est toujours à portée de main faciliterait aussi une utilisation journalière liée aux paiements.

---

[32] Le taux de pénétration du GSM en Europe de l'Ouest était supérieur à 60% en 2001 (Association GSM, mai 2001)
[33] L'équipement informatique des ménages est d'environ 60% et à peine 43% des ménages se connectent régulièrement à Internet, ILReS - Plan d'action eLuxembourg 2001
[34] Site web cellular-news le 22-Mar-2002, Report: Micro payments through cellphones would be used
[35] Retail electronic payments, David Birch, in "E-money and Payment Systems Review ", Central Banking Publications, 2002

Pour être pris en considération, un instrument de paiement mobile devra être sûr. D'une manière générale, l'instauration de labels de sécurité pour informer les consommateurs quant au niveau de sécurité peut être envisagée pour promouvoir et renforcer l'adoption d'un instrument de paiement.

3.1.3.2.2 Pression commerciale

La question du paiement mobile se pose déjà pour le téléchargement de logos, sonneries et autres services à valeur ajoutée. Ce type de prestation est actuellement offert et facturé via un numéro d'appel ou un SMS à tarification surtaxée. Ces numéros spéciaux ne sont en général pas accessibles aux visiteurs étrangers, supprimant ainsi une source de revenus.

La valeur du commerce mobile mondial est estimée à 100 milliards de dollars à l'horizon 2006[36]. Ces prévisions alléchantes incitent aussi bien les équipementiers, les fournisseurs de services, les commerçants, les portails mobiles, les opérateurs de téléphonie mobile que les banques à proposer et/ou à stimuler le développement de solutions de paiements mobiles en ligne.

Les développements espérés de l'UMTS -*Universal Mobile Telecommunications System*- en matière d'accès Internet et de son corollaire, le commerce mobile, rendront la question du paiement mobile plus complexe. L'offre de biens et de services proviendra d'un nombre beaucoup plus élevé de commerçants et de portails. Certains services à usage immédiat (typiquement l'achat de pages d'informations, de tickets de cinéma ou par un distributeur automatique) exigeront un paiement avec une confirmation sans délai. Dans les autres cas, la possibilité de paiement synchronisée à la commande se justifie pour le renforcement de la transaction commerciale. La pluralité des instruments de paiement est acquise par les consommateurs, et doit donc être intégrée dans les solutions de paiement mobile. Néanmoins, il faut veiller à ce que la multiplicité des canaux ne porte à confusion.

3.1.3.2.3 Possibilités technologiques

La carte à puce est présente dans le domaine des paiements. Elle est aussi utilisée sous un standard différent dans la norme de téléphonie mobile européenne, le GSM[37] -*Global System for Mobile Communication*-. La combinaison des deux est une possibilité techniquement réaliste pour les paiements mobiles, par exemple dans le projet Carte Bleue sur mobile en France[38]. Un terminal mobile peut être modifié pour pouvoir lire d'autres puces que la SIM[39] -*Subscriber Identity Module*- et faire fonctionner des applications de sécurité: vérification de PIN -*Personal Identification Number*-, signature électronique, etc.

Les canaux de communication sans fil ne sont pas restreints uniquement au transport de la voix. Les réseaux actuels permettent déjà l'échange crypté de données et de SMS et assurent une confidentialité qui est d'autant plus importante lorsqu'il s'agit de données bancaires ou de paiement. Ils peuvent aussi prendre en charge la reconnaissance de codes PIN lors d'une

[36] The Yankee Group, cité par Hallsenius Johan, BrainhHeart Magazine, The Virtual Bank 2002: Operators Lead the Way but Banks will Prevail, April 2002
[37] Voir Annexe 2
[38] Cette solution fonctionne sur un téléphone bi-fentes, un lecteur de carte à puce pour la carte SIM et l'autre pour la Carte Bleue.
[39] Voir Annexe 3
[40] Voir Annexe 2

communication. Outre le spectre radioélectrique de la norme téléphonique, un téléphone peut être équipé de fonctionnalités infra rouges et Bluetooth[40] pour communiquer sans fil et sans devoir établir de communication payante (WAP -*Wireless Application Protocol*-, SMS ou voix) avec un terminal de vente. Les développements de carte à puce sans contacts vont en ce sens.

Les autres terminaux mobiles peuvent aussi être équipés de ces fonctionnalités pour effectuer des paiements nomades plutôt que mobiles.

Le caractère mobile de ces terminaux les rend adaptés aux transactions P2P (de personne à personne) et à tous les types de commerce: face à face en magasin, Internet, à distance, distributeurs automatiques. Grâce aux accords de *roaming*[41], les solutions de paiement mobile pourraient même être accessibles en dehors du territoire national. En outre, ils sont autonomes et complets en permettant d'engager un paiement et de le valider, ou seulement de le confirmer en complément à un autre canal de transmission du paiement.

3.1.3.3 Exemples de solutions de paiement mobile

Les solutions de paiements mobiles ont fait leur apparition dans les années '90. Depuis, les offres touchant aux paiements à l'aide d'un terminal mobile se sont multipliées de façon très diversifiée. Les quelques exemples qui suivent en sont la démonstration.
L'échantillon repris ici est centré sur l'Union européenne pour des raisons d'homogénéité (norme GSM, cadre légal, ...). Mais l'Europe n'est pas la seule région du monde active dans les solutions de *m-payments* et de *m-banking*. On peut citer par exemple le *m-banking* de Singtel Mobile en collaboration avec la United Overseas Bank et la Development Bank of Singapore à Singapour, les paiements mobiles de Smart Communications aux Philippines et de Fundamo en Afrique du Sud et les plans de l'opérateur Sprint de constituer un réseau de paiements mobiles à travers les Etats-Unis.

[41] Voir Annexe 2

Nom du système	A. Participants	B. Instrument de paiement	C. Usages
1. Paybox (U.K.)	Le système est exploité par Paybox. Ses partenaires incluent, entre autres, la Deutsche Bank qui assure un accès aux systèmes de compensation. Paybox est d'origine allemande. Son déploiement s'étend au Royaume-Uni, en Autriche, en Espagne et en Suède.	Débit direct du compte courant du client par ordre de Paybox. Le client signe préalablement une autorisation de débit. Une limite de crédit est calculée en fonction des données bancaires du client. Règlement effectué par BACS (système de paiement de masse britannique)	Confirmation de paiement pour les achats Internet et en magasin, transfert P2P vers un autre numéro de mobile membre du système (tous pays) et demande de fonds à un autre numéro de mobile.
2. Sonera Shopper	Sonera (premier opérateur de téléphonie mobile en Finlande avec 60% de part de marché)	Cartes Visa et Eurocard ou le compte Sonera Shopper (compte individuel lié au numéro d'appel que le propriétaire approvisionne par avance)	Achats en magasins et à distance (y compris par Internet)
3. M-pay bill	Europolitan, opérateur GSM suédois (détenu à 71% par Vodafone, 50 millions de clients en Europe)	Compte prépayé ou compte de crédit auprès d'Europolitan.	Micro-paiement des achats sur le portail mobile de Europolitan. Ce service de paiement sera par la suite étendu pour les achats en magasins.

D. Transaction de paiement	E. Coût d'utilisation du service pour l'utilisateur	F. Réglementation	G. Degré d'ouverture du système
Le client donne son numéro de mobile (ou l'alias de confidentialité) au caissier qui le transmet au serveur Paybox. Le client est appelé sur ce numéro pour lui indiquer le montant et le bénéficiaire du paiement. Il confirme la transaction en entrant son code PIN. Les deux parties reçoivent une confirmation de la transaction.	La réception des appels est gratuite sur les réseaux GSM en Europe. Le montant annuel de l'abonnement est GBP 9,99.	Aucune réglementation bancaire spécifique car le système fonctionne toujours en collaboration avec un organisme bancaire. Fonctionne sur un modèle similaire aux organisations de cartes de crédit: les commerçants paient une commission de transaction et un abonnement annuel.	Accepte les abonnés de tous les réseaux GSM de chaque pays couvert. 500 000 clients[42] et plusieurs milliers de sites Internet et magasins adhérents pour l'ensemble de l'Europe. L'utilisation du système n'est possible que dans le pays d'inscription. Seuls les résidents peuvent y adhérer.
Le client envoie un SMS à la plate-forme Sonera et s'authentifie par son PIN. La plate-forme renvoie au client un code identitaire (6 chiffres) de paiement qui est valable 30 minutes et à communiquer au commerçant. Ce dernier renvoie à la plate-forme son identité, ce code identitaire et le montant du paiement. Le commerçant et le client reçoivent une confirmation de la transaction.	L'envoi du SMS est facturé 0,16 euros.	Pas de licence bancaire car aucun intérêt n'est payé sur le solde du compte Sonera Shopper.	Les abonnés des autres réseaux peuvent souscrire au service de paiement par carte de crédit. 31 chaînes de magasins acceptent ce mode de paiement. Seuls les paiements nationaux sont possibles, leur accès est limité au territoire et aux résidents finlandais.
Numéro d'identification (qui correspond au numéro de mobile) et PIN à utiliser pour la confirmation de paiement d'une transaction.		Pas de licence bancaire car les crédits sont remboursés endéans les 30 jours.	Les abonnés des autres réseaux suédois peuvent participer au système par un compte prépayé (seulement possible pour les résidents). Nécessite les fonctionnalités WAP.

[42] European Card Review, janvier/février 2002

Nom du système	A. Participants	B. Instrument de paiement	C. Usages
4. Mobipay (Espagne)	Résultat de la fusion des systèmes concurrents Movilpago et Pagomovil développés par Telefonica Moviles et Airtel Vodafone, tous deux opérateurs de téléphonie mobile, en coopération avec plusieurs établissements de crédit. L'alliance est maintenant ouverte et regroupe 100% des opérateurs de téléphonie mobile et environ 60% des émetteurs de cartes de paiement et les 3 systèmes de paiement nationaux.	Carte de débit, carte de crédit ou compte prépayé.	Paiement d'achats en magasin, à un distributeur automatique, sur Internet. Transferts P2P et rechargement de la carte téléphonique prépayée.
5. m-bankieren (Pays-Bas)	La banque de la poste Postbank, en association avec l'opérateur de téléphonie O2 (anciennement Telfort).	Les virements par un accès direct au compte.	M-banking: vérification du solde du compte, transferts, demande de cours boursiers.
6. E-ticketing (Finlande)	Les opérateurs nationaux et un opérateur estonien de téléphonie mobile.	Carte de téléphonie prépayée ou facture, payable par un instrument de paiement habituel.	Achat de tickets de bus de la ville de Helsinki dématérialisés (sous forme de SMS).

D. Transaction de paiement	E. Coût d'utilisation du service pour l'utilisateur	F. Réglementation	G. Degré d'ouverture du système
Le client reçoit un code barre, qui est collé au dos du téléphone. Le magasin scanne le code barre du client et introduit le montant à payer dans son système qui envoie au client un SMS de confirmation. Le client autorise le paiement par son code PIN. Après vérification, une confirmation de transaction est envoyée au client et au commerçant.	Aucun.	Les établissements bancaires sont des participants actifs de l'alliance. Aucune réglementation supplémentaire n'est applicable.	Le système n'est pas accessible depuis l'étranger ni aux visiteurs occasionnels.
Gestion du compte en accédant à une page WAP. Le numéro d'appel permet d'identifier le client et de le diriger directement vers son compte. L'authentification s'effectue par un code PIN dédié (le m-code).	Les services eux-mêmes sont gratuits, les coûts de communication d'accès au site sont de 0,20 euros par minute (le tarif normal WAP).	Aucune réglementation supplémentaire n'est applicable car les services sont les activités bancaires déjà exercées par Postbank.	Le service n'est accessible qu'aux clients O2 prépayés. Pas de paiement en ligne (exception faite du rechargement de la carte prépayée de téléphone via le compte) ni en magasin. L'accès en roaming à un site WAP est encore aléatoire.
Envoi d'un SMS vers un numéro surtaxé. Le SMS reçu en retour est la preuve du ticket de bus à présenter au contrôleur qui peut en vérifier la validité en interrogeant un serveur.	Pas de coût causé par la mobilité. Ce serait plutôt le contraire: le ticket est moins cher par SMS (1,40 euros) que le ticket physique (1,90 euros).	La réglementation sur les établissements de monnaie électronique ne s'applique pas car le compte ne peut servir que chez un commerçant.	Le numéro de SMS surtaxé n'est pas accessible aux visiteurs occasionnels (exception faite de l'opérateur estonien).

Nom du système	A. Participants	B. Instrument de paiement	C. Usages
7. Paiement CB sur mobile	Le Groupement des Cartes Bancaires et les trois opérateurs nationaux de téléphonie mobile.	Carte de débit, carte de crédit ou compte prépayé.	Paiements par carte en magasin ou à distance (minitel, Internet, catalogues).
8. clic paiement	Orange France, opérateur téléphonique.	Compte prépayé lié au numéro d'appel, rechargeable par une carte prépayée ou une carte bancaire (si le client est affilié au service "Paiement CB sur mobile").	Micro-paiement (max. 10 euros) de services d'éditeurs en ligne (WEB ou WAP) et de kiosques vocaux commercialisés par Orange.
9. Vodafone m-pay	Vodafone D2, Allemagne	Carte téléphonique prépayée ou report sur la facture téléphonique mensuelle.	Micro paiements (max. 10 euros) pour le commerce mobile et les achats Internet.

D. Transaction de paiement	E. Coût d'utilisation du service pour l'utilisateur	F. Réglementation	G. Degré d'ouverture du système
Le client appelle le commerçant avec son mobile pour passer commande. Le commerçant se connecte à sa plate-forme de commerce mobile pour envoyer au client un SMS de confirmation et de demande de paiement. Le client insère sa carte bancaire dans le second lecteur de son mobile et s'authentifie par PIN. Le terminal mobile envoie automatiquement un SMS de demande d'autorisation au gestionnaire des cartes de paiement. Après vérification et validation, une confirmation de transaction est envoyée au commerçant et au client. Le commerçant ne prend jamais connaissance du numéro de carte du client.	Le SMS de demande d'autorisation, dont coût en fonction de la tarification des réseaux.	Aucune disposition supplémentaire particulière n'est à respecter. La gestion des cartes de crédit fait partie des activités de base du groupement CB.	Seuls les titulaires d'une carte émise par le groupement CB peuvent faire usage du système. Il est disponible au client lorsqu'il se trouve à l'étranger. Les visiteurs occasionnels ne peuvent faire usage de ce système. Nécessite un téléphone bi-fentes spécifique.
Le client confirme son achat et le paiement par un code PIN. Le compte prépayé est débité par l'identification du client par son numéro d'appel.	Aucun coût n'est lié à l'usage du service. La vérification du code PIN se fait en ligne lors de la communication établie pour l'achat.	La réglementation sur les ELMI n'est pas d'application car la e-monnaie n'est acceptée que pour le paiement de services fournis et commercialisés par l'émetteur lui-même.[43]	Système propriétaire à Orange. L'accès WAP en roaming est possible, mais encore limité.
Achat sur le portail WAP de D2: le client clique la validation du paiement et D2 confirme automatiquement la transaction. Achat Internet: le client choisit la solution de paiement Vodafone D2, il reçoit par SMS un code de paiement qu'il donne au commerçant Internet pour confirmation de paiement.	Aucun.	Aucune réglementation bancaire spécifique n'est d'application. Vodafone D2 prend la responsabilité totale du paiement des partenaires commerçants.	Seuls les abonnés de Vodafone D2 bénéficient de ce système. Aucune démarche d'inscription pour l'abonné, il peut utiliser le service à tout moment.

[43] A terme, Orange France compte ouvrir ce service à des contenus de tiers impliquant une possible application de la directive sur les ELMI. Source informelle Orange France.

Le terme de "paiement mobile" recouvre donc une foule de possibilités:

- Accès aux services bancaires à distance
  C'est une application de l'*e-banking*.
- Canal séparé de confirmation du paiement
  L'opérateur téléphonie n'intervient pas dans le paiement à proprement parlé.
- Déduction d'un compte de paiement prépayé
  C'est une forme de monnaie électronique.
- Report du paiement sur la facture mensuelle
  Un crédit est accordé à l'abonné.
- Déduction du paiement de la carte téléphonique prépayée
  C'est une variante de monnaie électronique.
- Utilisation d'un porte-monnaie électronique émis par une tierce partie
- Rechargement des cartes téléphoniques prépayées
  Débit du compte sans passer par un guichet automatique de retrait.
- Activation d'un instrument classique de carte de crédit
  Le téléphone sert de borne de paiement, ou POS - *Point-Of-Sale*.

3.1.3.4 Caractéristiques et modèles

Les exemples repris ne reflètent pas les développements incessants, notamment par de nouvelles applications technologiques, comme les transmissions par Bluetooth ou par infrarouge, qui permettent l'échange de données entre une carte à puce et un terminal de vente sans contact physique, sans autorisation du gestionnaire du réseau de communication et sans devoir établir de communication payante. Eurocard a testé une solution de téléphone mobile Bluetooth en Suède en 2001.

Notre échantillon est assez restreint mais permet tout de même de mettre en évidence les nombreuses alternatives du point de vue des intervenants et de leurs rôles, des instruments de paiement et des configurations. Les différences fonctionnelles et technologiques ne sont pas étudiées dans ce cadre.

3.1.3.4.1 Participants

S'agissant de paiements échangés par un réseau de communication sans fil, les participants principaux sont les opérateurs de téléphonie mobile. Plus précisément en ce qui concerne le traitement des paiements, leur participation est en général partagée avec une banque ou un émetteur de cartes de paiement. Mais elle est parfois exhaustive, Orange France traite seul du paiement dans "clic paiement". La participation peut aussi se faire sans intervention dans les paiements, les réseaux mobiles servent uniquement de support de transmission dans Paiement CB sur Mobile et n'opèrent aucune fonction spécifique aux paiements.

Comme il s'agit de paiements, la participation d'établissements de crédit est tout à fait cohérente. Leur concours est utile pour l'accès aux systèmes de paiement et de règlement, il se justifie lorsque l'activité envisagée requiert un agrément bancaire. Partant d'un raisonnement similaire pour l'accès aux réseaux des cartes de crédit, la participation des émetteurs et gestionnaires de cartes est pertinente.

Mais l'établissement bancaire ne participe pas toujours au paiement lui-même. Par exemple, dans l'initiative paybox l'autorisation et la confirmation de paiement sont faites par paybox. Les établissements bancaires interviennent par la suite pour le règlement.

3.1.3.4.2 Instruments

Les instruments de paiement dénombrés sont les cartes de crédit et de débit, le débit direct, le débit du compte bancaire prépayé dédié ou du compte prépayé, et les virements via le *m-banking*.

A l'exception du compte prépayé, apparenté à de la monnaie électronique, les paiements mobiles reposent sur des instruments de paiement scripturaux existants. C'est une déduction identique à celle déjà établie pour les paiements électroniques.

Dans tous les cas de figure, il n'y a pas de nouveauté en matière de règlement. Quels que soient les canaux d'accès, mobiles, électroniques ou autres, le règlement s'effectue par le biais de systèmes de compensation et de règlement bancaires.

Un lien existe entre l'instrument de paiement utilisé et la qualité du ou des prestataires. La réglementation relative à un instrument de paiement détermine les exigences quant au type d'établissement qui peut l'émettre et le gérer et qui devra donc faire partie des prestataires ou être le seul prestataire. Par exemple, un système de monnaie électronique non restrictif nécessite un ELMI. C'est une des raisons qui explique la coopération entre établissements de crédit et les opérateurs dans la fourniture de services de paiements mobiles.

3.1.3.4.3 Configuration: concurrence ou coopération?

Les solutions pour les micro-paiements passent principalement par le débit d'un compte prépayé ou le report sur la facture (impliquant un risque débiteur pris en charge par l'opérateur téléphonique). Les cartes de paiement et les comptes dédiés ou bancaires sont plutôt utilisés pour les paiements de montant plus important.

Face aux possibilités et aux restrictions de chaque instrument, les prestataires peuvent choisir d'offrir plusieurs solutions de paiement mobile: un instrument pour les micro-paiements (compte prépayé ou dédié) et un instrument bancaire pour les montants plus élevés. A l'instar de Orange France qui propose "clic paiement" et "Paiement CB sur mobile". Une telle structure reflète aussi le risque pris par les intervenants (l'opérateur dans le premier cas et la banque dans le second).

Selon les instruments de paiement mis en œuvre, l'intervention d'un établissement de crédit, d'un ELMI ou d'un émetteur de cartes de paiement peut s'avérer obligatoire tant pour les micro-paiements que pour les montants plus élevés. De fait, une majorité de solutions de paiement mobile présente un profil de coopération entre établissements de crédit et opérateurs téléphoniques. Par ailleurs, une étude ePSO[44] constate que la majorité des projets de paiements électroniques interrompus n'implique pas de banques et que les nouveaux projets les incluent. Cette présence prédominante n'est pas particulièrement visible aux clients car la banque ne constitue pas toujours l'interface entre le client et sa solution de paiement mobile. Elle intervient pour les autorisations, les confirmations et les règlements; l'opérateur sert d'interface électronique pour les paiements.

[44] ePSO background paper 9

Plutôt que la concurrence, la coopération entre les banques (ou les émetteurs de cartes) et les opérateurs est préférée car elle permet de tirer des synergies des avantages comparatifs de chacun, de réduire les coûts et de mettre en place des standards intersectoriels pour le marché. Ensemble, ils peuvent jouer sur leur positionnement transfrontalier (réseau bancaire, réseaux de cartes ou accords de *roaming* international pour le GSM) pour offrir des solutions internationales de paiements mobiles.

Chacun des intervenants a de bonnes raisons et de bons atouts, mais présente aussi des désavantages pour pouvoir assumer seul le déploiement et la gestion d'une solution.

Opérateurs de téléphonie mobile

Les opérateurs de téléphonie mobile ont commercialement tout intérêt à développer les paiements mobiles afin d'augmenter les revenus liés au commerce mobile (commissions d'intermédiation, facturation du temps de connexion et des téléchargements).

Ils se basent sur l'expérience acquise dans la facturation de petits montants, la re-facturation (le *roaming* international est une activité maîtrisée qui comporte la facturation de services tiers) et la gestion des comptes prépayés. Ils ont l'avantage de pouvoir réagir très rapidement car ils sont soumis à moins de contraintes réglementaires que les banques.

Cependant, leur vision pourrait être trop orientée sur le court terme car la plupart des opérateurs GSM (en Europe et ailleurs) connaissent des inquiétudes financières suite aux investissements élevés dans les réseaux de 3ème génération[45] (UMTS) pour l'obtention de la licence et les équipements à mettre en place selon un échéancier décidé par les autorités de télécommunications.

Leur plus grand désavantage est le manque d'expérience dans les services de paiement, surtout si ceux envisagés sont soumis à une réglementation bancaire. Leur approche de la gestion des risques devra faire face aux changements des risques issus de la gestion des paiements de masse et des conventions financières avec les commerçants. Ils doivent justement prendre des accords commerciaux avec ces derniers, à moins de s'allier à des gestionnaires de cartes de paiement dont le réseau commercial s'est mis en place au cours des années.

Etablissements de crédit

Les établissements de crédit dominent traditionnellement le secteur des paiements. Ils se doivent de participer au développement de paiements sans fil sous peine d'un risque de désintermédiation en faveur de nouveaux intervenants non bancaires.

Ils ont un avantage certain en ce qui concerne la gestion des crédits, les paiements de masse et les services financiers s'y rapportant. En outre, ils sont inévitables pour le règlement et ont une relation déjà bien établie avec les émetteurs et gestionnaires de cartes de crédit.

Leur élan innovateur pourrait être bridé par une certaine lenteur de réaction, notamment en raison du cadre réglementaire bancaire et d'un accès indirect aux services mobiles.

[45] Voir Annexe 2

Emetteurs de cartes de crédit

L'intérêt des émetteurs et gestionnaires de cartes de crédit dans la participation aux solutions de paiements mobiles réside dans le risque de désintermédiation et dans les possibilités de nouveaux canaux d'accès qu'offre le terminal mobile.

Sans vraiment posséder des capacités efficaces pour la facturation de petits montants, ils ont cependant acquis une bonne expérience en matière de services et de règlement financiers. Ils ont surtout réussi à développer un réseau étendu de commerçants partenaires au fil des années.

Entrepreneurs non bancaires

Sans nécessairement être une banque ou un opérateur de téléphonie, une entreprise peut s'investir dans un créneau de paiements mobiles.

Certaines ont un intérêt plus marqué grâce à leurs liens avec les paiements par Internet ou avec les réseaux de communication sans fil. On peut mentionner entre autres:

- Les portails Internet généralistes (Yahoo !)
  Leurs services de paiement en ligne sont extensibles aux paiements mobiles.
- Les portails spécialisés en services mobiles (Aladdino, Aspiro, go mobile…)
  Le commerce mobile est une motivation forte au développement des paiements mobiles.
- Les fournisseurs de contenu (Reuters)
  Ils sont directement intéressés par la vente et le paiement de leurs services.
- Les chambre de compensation de téléphonie mobile (MACH, Dannet)
  Leur intervention dans la compensation et le règlement des données de communication peut s'étendre aux données de facturation et de paiement avec les commerçants et/ou les banques.
- Les équipementiers.

Ils ont l'avantage d'une présence mondiale et de participer aux accords de standardisation.

Leurs chances de succès en procédant isolément sont considérées comme assez limitées à cause du cumul des désavantages des banques et des opérateurs, principalement l'accès indirect aux plates-formes mobiles, l'inexpérience en matière de paiements de masse (sauf pour les prestataires de paiements sur Internet), l'inexistence d'un réseau de commerçants affiliés et une vision à court terme. De plus, ils ne disposent pas de leur propre base de clients, contrairement aux banques et aux opérateurs qui peuvent s'appuyer sur une clientèle passablement captive pour un service lié à leurs activités de base.

Cependant, leur offre de services ne serait pas limitée aux clients d'un opérateur ou d'un établissement de crédit. Ces entrepreneurs pourraient réagir très rapidement.

3.1.3.5 Cadre réglementaire

Malgré l'ampleur et les montants actuellement insignifiants des paiements mobiles, les autorités peuvent décider d'intervenir et de soumettre certaines activités traditionnellement bancaires à des vérifications préalables. Notamment sur des dispositions de sécurité, en vue de protéger les consommateurs.

La prise en compte des pratiques et des objectifs de sécurité spécifiques aux réseaux sans fil au sein des normes de supervision bancaire va en ce sens. L'autorité monétaire de Singapour,

Monetary Authority of Singapore, a l'intention d'inclure la version finale de ses *Security Guidelines for Mobile Banking & Payments*[46] parmi ses exigences de supervision applicables aux établissements financiers qui offrent des services de paiements mobiles et d'accès bancaire mobile.

Des conditions préalables existent déjà en ce qui concerne certains instruments de paiement. La gestion d'un compte bancaire requiert la qualité d'établissement de crédit.

Un compte prépayé (géré par les opérateurs dans les exemples qui précèdent) servant au paiement d'achats auprès de fournisseurs différents entre dans la définition légale de la monnaie électronique: support électronique, remise de fonds égale à la valeur monétaire émise et acceptation comme moyen de paiement dans d'autres entreprises que l'émetteur. Ce dernier doit se soumettre à un agrément d'établissement de monnaie électronique. C'est le cas au Grand-Duché de Luxembourg pour les non-banques.

Outre l'acceptation très limitée de la valeur monétaire électronique permettant de déroger à cette réglementation[47], certaines exemptions sont prévues dans la directive 2000/46/CE[48]. Mais l'applicabilité des possibilités d'exemption est décidée au niveau national et leur substance est inconnue. Au Grand-Duché de Luxembourg, la CSSF en décide sur base d'une demande écrite. Une incertitude subsiste aussi en ce qui concerne l'utilisation des cartes téléphoniques prépayées. Le montant versé par avance par le client à l'opérateur sert à priori au paiement des communications. Si la possibilité de payer d'autres fournisseurs est donnée au client, il est difficile de prévoir d'avance la proportion qui sera allouée à la téléphonie de celle impartie à des paiements de tiers, et donc à considérer comme de la monnaie électronique. Comment l'opérateur pourrait-il adhérer correctement à la législation (par exemple pour les données statistiques et la constitution des réserves obligatoires) et le cas échéant faire valoir ses possibilités d'exemption, si ce n'est qu'après l'utilisation de la valeur prépayée? Considérer la totalité des montants prépayés comme de la monnaie électronique, avec toutes les restrictions s'y rattachant, est pénalisant pour la partie finalement consacrée à la téléphonie. Les opérateurs GSM[49] se penchent sérieusement sur ces indéterminations réglementaires et les risques qui en découlent.

On peut néanmoins considérer le cadre réglementaire concernant l'instrument de monnaie électronique comme étant plutôt uniforme au niveau de l'Union européenne. Les activités bancaires et la provision de services de paiements sont soumises à des dispositions nationales plus fragmentées. Dans certains Etats membres, l'émission d'instruments de paiement (par exemple le crédit consistant au paiement d'un fournisseur tiers par une facturation ultérieure à l'achat) n'est pas synonyme d'activité bancaire. En revanche, d'autres la considèrent comme telle et la soumettent à une licence bancaire[50]. Au Grand-Duché de Luxembourg, l'octroi de crédits pour des biens de consommation n'est pas sujet à un agrément de PSF si l'activité de crédit n'est pas exercée à titre principal (au-delà de 50% du chiffre d'affaires).

La gestion des autorisations des cartes de crédit est dans la pratique du ressort des banques émettrices. Elle peut se faire en coordination avec les émetteurs de cartes et les gestionnaires

[46] Le document a fait l'objet d'une consultation publique.
[47] Situation actuelle de clic paiement en France.
[48] Voir le paragraphe sur La législation européenne pour plus de détails.
[49] White Paper on Micro-Payments, GSM Association
[50] Lelieveldt Simon, ePSO-Newsletter - Nr. 1 - juillet 2000

des réseaux de cartes. L'émission d'instruments de paiement tels que les cartes de crédit n'est pas soumise à un agrément ni à une supervision au Grand-Duché de Luxembourg.

3.1.3.6 Incertitudes pour les paiements mobiles

Outre les incertitudes légales que l'on vient de présenter, des doutes subsistent quant aux déploiements commerciaux et techniques des nouveaux réseaux sans fil. L'UMTS prend beaucoup de retard sur le terrain. Des reports de déploiement ont même été demandés par des détenteurs de licence. En fait, seuls 10% des utilisateurs de téléphone mobile de l'Europe de l'Ouest passeraient à l'UMTS à l'horizon 2007[51].

Des disparités mondiales dans les conditions de marché freinent l'émergence de standards. En comparaison avec l'Europe, le Japon a acquis une avance dans le commerce mobile et les réseaux de troisième génération, les Etats-Unis sont pénalisés par la multiplicité des normes déployées. Même dans les pays regroupés au sein d'une norme unique de téléphonie mobile, l'émergence d'un standard ou de standards compatibles pour les paiements est lente et difficile. Plusieurs modèles[52] (téléphone bi-fentes, signature électronique, PIN, etc.) sont techniquement réalisables.

En plus des conditions de réussite du commerce mobile et de l'émergence de standards, les paiements mobiles ne connaîtront un succès que s'ils sont accessibles à partir de n'importe quelle localisation, même à l'étranger. Nous sommes tous habitués aux bénéfices des services du *roaming* en téléphonie mobile et attendons la même ubiquité pour les paiements mobiles.

3.2 Spécificités des instruments de paiement électronique

Au-delà des caractéristiques communes entre les paiements scripturaux et les paiements électroniques, les exemples repris ci-dessus soulignent des éléments distinctifs assez importants pour justifier une approche adaptée de politique de sécurité:

1. Les instructions en relation avec les paiements électroniques de masse sont transmises par l'intermédiaire de réseaux ouverts (Internet, téléphone, réseaux sans fil…).

Les réseaux ouverts engendrent une identification plus difficile des intervenants. Des mesures permettant l'identification et l'authentification des parties en présence existent et doivent être appliquées au domaine des paiements: PIN, signature électronique, …[53]

Les réseaux ouverts n'ont pas été conçus pour assurer la confidentialité et l'intégrité des données qu'ils transmettent. Des outils mathématiques de cryptographie et de contrôle de parité sont appliqués afin de pourvoir à ces exigences.

La propagation d'une défaillance est moins contrôlable et par conséquent plus rapide au sein d'un réseau ouvert.

2. L'intervention de prestataires de services sans expérience dans les paiements.

Cette intervention est facilitée par les réseaux ouverts et l'adaptation du cadre réglementaire.

---

[51] Forrester Research, Octobre 2002
[52] Voir Annexe 2
[53] Voir Annexe 3

Dans un domaine qui n'est pas familier aux nouveaux intervenants et qui a trait à la monnaie et à la confiance du public, des mesures de prévention et une surveillance similaire à celle appliquée aux établissements de crédit peuvent s'avérer nécessaires et sont par ailleurs prévues.

3. L'obligation de pouvoir retracer des transactions.
L'usage de la monnaie électronique ne donne pas lieu à l'impression d'extraits de compte. La remboursabilité de la monnaie électronique étant légalement obligatoire, même en cas de destruction du support de la monnaie, des mesures doivent être prises pour pouvoir calculer le solde d'un porte-monnaie et ainsi assurer la traçabilité au sein du système.

De la manière similaire, tout transfert de fonds effectué au moyen d'un instrument de paiement électronique doit pouvoir être retracé sur une période de trois ans au Grand-Duché de Luxembourg.

4. L'intervalle de temps entre l'émission du paiement et son autorisation est plus court.
S'agissant de soutenir ou simplement de servir le commerce en ligne électronique ou mobile, le laps de temps entre l'émission du paiement et sa confirmation (au payeur et au bénéficiaire) se doit d'être le plus court possible.

Les systèmes doivent donc minimiser la probabilité d'une défaillance et la durée d'une indisponibilité.

5. La dépendance accrue par rapport aux TIC (technologies de l'information et des communications).
Les paiements électroniques signifient intrinsèquement un traitement électronique de bout en bout des transactions. Cela implique que celles-ci sont totalement dépendantes d'infrastructures technologiques.

Par ailleurs, la tendance des établissements de crédit à sous-traiter les fonctions secondaires (traitement des données, gestion des guichets automatiques et des terminaux en magasin...) pour des raisons de recentrage des activités et d'économie d'échelle, augmente la concentration des risques opérationnels sur un nombre plus limité d'infrastructures technologiques.

Ces risques opérationnels sont pris en compte dans une politique de sécurité.

3.3 Risques associés aux instruments de paiement électronique

Ces différences entre les paiements électroniques et les paiements scripturaux tendent à indiquer que certains risques sont de nature différente ou de nature identique mais de niveau différent.

La Banque des Règlements Internationaux (BRI) a identifié huit risques pour l'e-banking[54]. Par analogie, ils sont applicables aux systèmes de paiement électronique:

1. Risque de crédit
Le risque qu'un participant au système soit incapable d'acquitter intégralement ses obligations financières au sein du système, au moment prévu ou ultérieurement.

[54] Electronic Banking Risk Management Issues for Bank Supervisors, Electronic Banking Group White Paper, October 2000

2. Risque de liquidité
Le risque qu'un participant au système ne soit pas capable d'acquitter ses obligations financières au sein du système au moment prévu, mais il est en mesure de le faire ultérieurement.

3. Risque opérationnel
Le risque que des défectuosités techniques ou des erreurs opérationnelles entraînent ou aggravent des risques de crédit ou de liquidité.

Le risque opérationnel prend de l'importance au vu la dépendance accrue de la technologie, les banques ou opérateurs de services doivent mettre en place des infrastructures permettant l'interopérabilité et assurant la sécurité, l'intégrité et la disponibilité de données.

4. Risque légal
Le risque que le cadre juridique inadéquat ou des incertitudes juridiques entraînent ou aggravent des risques de crédit ou de liquidité.

La question du risque légal peut survenir dès lors que des non-banques interviennent dans les paiements et les règlements, en coopération avec des établissements de crédit ou seules par l'application de nouvelles dispositions dont des différences d'interprétation peuvent mener à des incertitudes.

5. Risque stratégique
Ce risque est plus spécifiquement lié aux nouvelles activités, telles que l'*e-banking* ou les nouveaux instruments de paiement. Ce risque est de nature plus générale et plus étendue. En effet, les décisions stratégiques quant aux nouveaux canaux d'accès et aux nouveaux services auront des conséquences sur les autres types de risque.

Les nouveaux instruments de paiement de masse font l'objet d'une stratégie de développement et de déploiement de la part des banques et des émetteurs de cartes de crédit, mais aussi de la part de la récente concurrence non-bancaire. Une offre trop en avance par rapport aux attentes des consommateurs risque de rendre le "nouveau" système obsolète au moment où le marché sera prêt. A l'inverse, un marché déjà saturé sera la réponse à un positionnement trop tardif. Dans les deux cas de figure, la situation financière et les autres risques s'en trouveraient impactés.

Pour les banques et les fournisseurs traditionnels de services de paiement, le risque stratégique est renforcé par un risque de désintermédiation où la concurrence non-bancaire parvient à déranger la relation classique entre une banque et son client. Si la position générale des banques s'en trouve affaiblie, il peut s'ensuivre une augmentation du risque de crédit et de liquidité.

6. Risque de réputation
Le risque de ternir sa réputation en cas de défaillance dans la sécurité, l'exactitude, la cohérence et la protection de données privées lors de la fourniture des nouveaux services de paiement.

7. Risque de règlement
Risque que le règlement n'ait pas lieu dans les conditions prévues.

Il est important de noter que jusqu'à présent, les nouvelles solutions de paiement utilisent les systèmes de règlement interbancaire existants[55]. Le risque de règlement est donc assez limité. Néanmoins, l'émergence de solutions par lesquelles le règlement du consommateur se fait par un compte non bancaire fait croître le risque de règlement et de finalité[56].

8. Risque de finalité
Risque qu'un transfert de fonds soit annulé par la suite.

Le risque peut dériver de l'absence de couverture par la loi définissant les conditions de la finalité d'un règlement. Par exemple, la participation d'un ELMI à un système de paiement soustrairait celui-ci de la couverture de la SFD.

3.4 Composantes de sécurité des instruments de paiement

Le niveau de sécurité d'un instrument de paiement est fonction de son cadre légal mais aussi de sa politique de sécurité technique et opérationnelle. L'adoption d'une telle politique nécessite la connaissance des risques techniques et opérationnels encourus et l'identification des composantes de sécurité.

Selon la politique de sécurité décidée, différents niveaux de sécurité seront mis en place pour chacune des composantes de sécurité. Pratiquement, la sécurité se base sur une combinaison de technique logicielle (le cryptage symétrique par exemple) et de support matériel (la carte à puce par exemple)[57]. Pour des raisons d'efficience globale, le niveau de sécurité réalisé ne sera pas nécessairement le niveau maximal techniquement réalisable.

La sécurité des paiements électroniques et d'une manière générale des transactions en ligne s'établit sur plusieurs composantes de sécurité, définies comme suit par l'Eurosystème[58]:

3.4.1 Disponibilité

Le système répond efficacement et dispose d'une capacité suffisante pour assurer un niveau de performance acceptable. Le service doit en outre être rapidement disponible suite à une interruption.

3.4.2 Authenticité

Le système est capable d'établir l'authenticité de l'identité de l'utilisateur et l'authenticité de l'autorisation de l'utilisateur. Il peut aussi assurer que toutes les transactions sont légitimes.

---

[55] "The majority of the new initiatives does not change the interbank settlement process, but use current systems, where settlement is effected through banks in the interbank payment systems.", BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002
[56] Personal On-Line Payments, Kenneth N. Kuttner and James j. McAndrews, FRBNY Economic Policy Review, December 2001.
[57] Voir Annexe 3
[58] BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002

3.4.3 Non répudiation

La méthode d'authentification utilisée doit permettre de prouver que le message de transaction a effectivement été envoyé et reçu. Ainsi, l'émetteur et le destinataire sont protégés contre toute rétraction de l'autre partie; la responsabilité de la transaction est bien établie.

3.4.4 Confidentialité

Le système prend les mesures nécessaires pour garantir la confidentialité de certains éléments de la transaction.

3.4.5 Intégrité

Le système applique les mesures appropriées aux fins de protéger l'intégrité des transactions. Toute information de passage ou stockée ne sera modifiée que sur autorisation.

L'utilisation des instruments de paiement par l'application de nouvelles possibilités technologiques dénote des risques et des composantes de sécurité différents. L'approche de la politique d'efficience et de sécurité doit être appropriée.

4 Futur des paiements électroniques

Les solutions de paiements électroniques, et par extension les paiements mobiles, n'ont pas encore véritablement percé. Elles suscitent néanmoins l'intérêt d'intervenants d'horizons très variés: opérateurs de téléphonie, entrepreneurs, portails, commerçants en ligne, équipementiers, banques, organisations sectorielles et organismes publics partout dans le monde. Les initiatives sont citées à titre d'exemple et ne sauraient constituer une liste exhaustive car leur nombre est trop important. Ces initiatives visent à promouvoir ces types de paiement et à établir des standards techniques et sécuritaires.

4.1 Conditions de réussite

Du point de vue des utilisateurs, les chances de succès de ces services reposent sur plusieurs critères:

1. Ubiquité
Le service est disponible partout à tout moment et offre les mêmes capacités.

2. Immédiateté
L'accès au service est direct et les transactions sont traitées immédiatement.

3. Continuité
Le service n'est pas lié à un nombre limité de prestataires de services ou de points d'utilisation. Le service est identique quel que soit le prestataire.

4. Facilité d'utilisation
Pour une assimilation plus rapide de la part des usagers.

5. Utilité réelle des services proposés
Le service répond à une demande réelle, plutôt qu'à un exercice technologique.

6. Sécurité des applications
Elle doit être perçue comme excellente par les utilisateurs.

7. Coût des services
Les consommateurs sont peu habitués à débourser pour pouvoir effectuer un paiement.

8. Surveillance et régulation
La surveillance et la certification par une autorité de régulation peut avoir un effet positif sur la confiance des utilisateurs.

4.2 Automatisation de bout en bout

Un traitement automatisé de bout en bout permet d'améliorer l'efficience des instruments et des systèmes de paiement.

Les plates-formes de paiements électroniques s'intègrent totalement dans l'optique d'un processus STP -*Straight Through Processing*- allant de l'EBPP -*Electronic Bill Presentment and Payment*- jusqu'à la réconciliation électronique. Chaque flux de la figure 1 dans le paragraphe Paiements électroniques est automatisable.

Les possibilités de facturation électronique dans le sens de l'EBPP ne sont pas pleinement exploitées. La directive européenne 2001/115/CE ouvre la voie de la facture électronique. Actuellement, les bénéfices de la facturation électronique sont restreints car l'acceptation en est encore très limitée et non obligatoire, contraignant les créditeurs à maintenir deux systèmes.

Certaines solutions EBPP offrent aussi des outils de réconciliation électronique, donc automatique, notamment grâce à un numéro de référence unique par transaction qui sera transmis tout au long du processus STP.

4.3 Initiatives des autorités

Les autorités publiques ont un intérêt clairement défini de promotion de la concurrence, de la sécurité et de l'efficience des instruments et des systèmes de paiement. Plusieurs initiatives ont été prises en matières de paiements électroniques. Certaines sont encore en cours.

4.3.1 Initiatives des institutions européennes

Le Conseil européen de Lisbonne a arrêté l'année 2005 comme échéance pour l'établissement d'un marché intégré des services financiers. Il reconnaît l'importance du renforcement de la confiance des consommateurs dans les paiements sur Internet. Cet objectif passe par la sécurisation des paiements électroniques et par un cadre législatif harmonisé garantissant le remboursement au consommateur en cas de problèmes. Ce point est souligné par la Commission[59].

[59] Commission des Communautés européennes, Communication de la Commission au Conseil et au Parlement: Commerce électronique et services financiers, 2001

L'intérêt de la Commission pour les paiements électroniques s'est notamment matérialisé par le projet ePSO *-Electronic Payment Systems Observatory-* qui a débuté en mai 2000 pour une période de deux ans. Ses objectifs étaient de:

- Constituer un inventaire des solutions de paiement électronique;
- Améliorer les échanges d'information en matière de paiements électroniques;
- Gérer un forum de discussion dans les domaines pertinents;
- Stimuler les discussions et les réflexions par l'édition de *ePSO-Newsletter* et de *background papers*.

Plus précisément en matière de paiements mobiles, depuis septembre 2002, la Commission européenne a pris l'initiative informelle d'élaborer un *blueprint* avec toutes les parties intéressées. La participation de la Commission dans cette initiative est celle d'un catalyseur neutre. Le but du document est d'aider le secteur à identifier les obstacles, établir les priorités, et si possible de trouver des solutions de commun accord, dans le développement des paiements mobiles. Les domaines de travail comprennent entre autres: la sécurité, le cadre légal et la standardisation. Une action concertée entre le secteur privé et les autorités est envisageable si le *blueprint* emporte une large adhésion.

En pratique, la Commission européenne a donné le coup d'envoi en juillet 2001 à son projet TELEPAY d'une durée de 18 mois. L'objectif est d'évaluer la faisabilité commerciale, technique et légale d'un système d'achat et de paiement de tickets électroniques en utilisant le SMS, l'accès WAP ou les possibilités de transmission sans fil de courte distance. Ce projet se base sur des déploiements réels sur le terrain. On peut citer par exemple les transports en commun de la ville de Berlin ou le péage dans la région de Dourdan au sud-ouest de Paris. Le rapport final a été publié en avril 2003. Il souligne la nécessité d'adapter et d'harmoniser le cadre légal pour les télécommunications et les paiements mobiles. D'autre part, il relève l'utilité d'étendre le service en *roaming*, de donner au consommateur plus de choix quant aux instruments de paiement et de développer les micro-paiements.

De son côté, le Conseil européen a "invité la Commission, les États membres et l'industrie à examiner les questions qui commencent à se poser concernant le commerce mobile et à aborder les éventuels problèmes de réglementation y afférents, par exemple dans des domaines tels que les systèmes de paiement mobiles".[60]

4.3.2 Initiatives récentes du SEBC et de la BCE

La Commission européenne et la Banque centrale européenne ont très récemment décidé de transférer l'ePSO à la BCE. La BCE a donné une nouvelle impulsion au site www.e-pso.info en mai 2003. C'est une démonstration de l'intérêt réel que le SEBC porte aux paiements électroniques.

L'annonce de ce transfert a été faite lors de la première conférence sur les paiements électroniques organisée par la BCE le 19 novembre 2002. Plus d'une centaine de participants ont pris part à cette *ECB Conference on E-payments in Europe*. La BCE se fonde sur son rôle dans la promotion du bon fonctionnement des systèmes de paiement pour contribuer à assurer la stabilité financière. L'inventaire des développements récents en la matière indique que le marché est assez fragmenté et encore à ses débuts. Les thèmes de la conférence étaient le futur

[60] Conclusions de la 2472ème session du Conseil- Transports, Télécommunications et Energie, Bruxelles, les 5 et 6 décembre 2002

des paiements électroniques, les obstacles à leur développement et les nouveaux prestataires dans le marché des paiements.

En 2002, la BCE a mené une consultation publique sur les objectifs de sécurité de la monnaie électronique. Le rapport "Electronic Money System Security Objectives" (EMSSO) a été publié le 23 mai 2003. Les objectifs de sécurité développés serviront à évaluer la fiabilité et la sécurité technique d'ensemble des systèmes de monnaie électronique.

Dans le cadre plus général des paiements de masse, l'Eurosystème a exercé son rôle de catalyseur au cours de l'année 2002 en initiant une consultation au sujet des normes de surveillance des systèmes de paiement de masse en euros. Il estime que six parmi les dix SIPS s'appliquent à certains systèmes de paiement de masse en euros.

4.3.3 Initiatives hors Union européenne

En dehors de l'Union européenne, les autorités monétaires prennent également des initiatives en matière de paiements électroniques et mobiles. On peut citer l'exemple de Singapour repris dans Cadre réglementaire concernant les paiements mobiles. En 2001, la *Monetary Authority of Singapore* avait déjà publié un document similaire pour l'*e-banking*, les *Internet Banking Technology Risk Management Guidelines*.

4.4 Initiatives du marché

Elles sont assez nombreuses et proviennent de secteurs différents (banques, télécommunications,...) ou sont le fruit d'approches intersectorielles. Ne sont ici repris que quelques exemples.

1. Mobey Forum (www.mobeyforum.org)
Le forum regroupe des banques et des fabricants de terminaux mobiles. Leur but est de promouvoir l'usage de la technologie sans fil dans les services financiers. Il propose une architecture de paiements mobiles indépendante[61] de l'opérateur et basée sur une carte à puce séparée émise par les banques.

La solution de *m-banking* développée par un de ses membres peut-être implémentée depuis le 30 juin 2003. L'utilisateur doit télécharger un logiciel qui lui permet de générer une signature électronique de type PKI.

2. MeT - Mobile electronic Transaction (www.mobiletransaction.org)
L'organisation regroupe des fabricants de terminaux mobiles et associe les institutions financières aux travaux. L'objectif est de créer un cadre technologique commun pour assurer la sécurité des transactions mobiles.

3. ECBS - European Committee for Banking Standards (www.ecbs.org)
Le comité regroupe les associations européennes des établissements de crédit.

Un comité technique est spécialisé dans les services électroniques. Son document *EBS602 electronic Payment Initiator* (ePI) daté de septembre 2002 a pour objectif de faciliter le STP.

[61] Mobey Forum, The Preferred Payment Architecture Executive Summary, Version 1.0, June 2001

Un de ses groupes de travail élabore un rapport sur les paiements mobiles, *DTR 603 Business and Functional Requirements for Mobile Payments*. La version 1 du document est disponible depuis février 2003. Son objectif est de faciliter la coopération des banques avec d'autres secteurs en définissant les exigences bancaires pour les paiements mobiles. Ainsi, les partenaires non bancaires peuvent développer la technologie adaptée et fournir des services de paiements mobiles sûrs et financièrement viables.

4. GSM Association (www.gsmworld.com)
L'association regroupe les détenteurs d'une licence GSM. Elle a publié un *White Paper on Micro-Payments* qui met en avant les questions légales, fiscales, pratiques et techniques de la mise en œuvre de micro-paiements mobiles.

5. Projet SmartEuro (www.eurosmart.com)
Le projet rassemble majoritairement des équipementiers et les fabricants de carte à puce à propos de l'interopérabilité des porte-monnaie électroniques.

4.5 La situation luxembourgeoise

Le Grand-Duché de Luxembourg a transposé la majorité des directives européennes favorisant le commerce et les transactions électroniques. L'intérêt du gouvernement luxembourgeois pour les opérations électroniques, échanges commerciaux et paiements, se reflète par le site étatique www.eluxembourg.lu. Par ailleurs, on peut citer à titre d'exemple le premier congrès international "e-commerce trustmarks" qui est organisé au Grand-Duché de Luxembourg par le Ministère de l'économie (l'OLAS et eLuxembourg)[62].

Cependant, peu de développements concernant les paiements électroniques ont lieu au Luxembourg. Le marché est limité et les établissements bancaires présents suivent les initiatives prises au niveau des maison-mères. A titre informatif, on peut signaler que la CSSF a établi un recensement au 31 décembre 2000 portant sur tous les établissements financiers établis au Luxembourg, à savoir 202 banques et 113 PSF. Sur les 85 sites Internet bancaires opérationnels, seuls 15 sont de type transactionnel. La proportion des sites permettant l'exécution de transactions et de paiements électroniques est assez faible.

La solution pay@cetrel déployée par le Cetrel prend en charge les paiements par carte de crédit sécurisés sur Internet.

Concernant plus spécifiquement les paiements mobiles, les conclusions d'une séance de la First Tuesday[63] indiquent qu'il est peu probable qu'une solution soit développée au Grand-Duché à moyen terme[64]. Les raisons avancées sont l'étroitesse du marché et un vide juridique relatif. Plusieurs intervenants, craignent notamment que l'implication de prestataires non bancaires et non surveillés par la CSSF dans les paiements constitue une brèche du secret bancaire. Ces entités ne sont en effet pas soumises aux mêmes obligations que les établissements de crédit.

---

[62] Il aurait dû se dérouler du 17 au 19 septembre 2003, mais il est annulé par manque de participants.
[63] Le 2 avril 2002
[64] Néanmoins, Tango permet le rechargement de ses cartes prépayées en utilisant une carte de crédit à partir du téléphone mobile, après signature d'une convention de m-commerce entre les deux parties. LUXGSM permet ce rechargement par un achat Internet payé par carte de crédit.

5 Conclusion

L'application de nouvelles technologies aux paiements de masse permet le déploiement de solutions de paiement innovantes. Pour autant, on ne peut pas conclure à de nouveaux instruments de paiement. En effet, ces nouvelles solutions se basent sur la monnaie électronique et en majorité sur des instruments de paiement scripturaux existants (cartes de crédit, virements, ...)

Une distinction existe pour la monnaie électronique. Son émission en dehors d'un cadre bancaire fait l'objet d'une réglementation européenne spécifique. Cette dernière gagne à être clarifiée si elle se veut être une opportunité pour des entrepreneurs non bancaires de participer aux paiements de masse. A la différence de la monnaie fiduciaire, la *e-money* n'est pas dotée du cours légal, sauf en cas d'émission par une banque centrale.

Les nouvelles solutions de paiement exploitent l'accessibilité des réseaux ouverts pour initier, transmettre et/ou confirmer des paiements. Parmi les réseaux ouverts, les réseaux de communication sans fil, typiquement la téléphonie mobile, constituent un choix pertinent pour une catégorie particulière de paiements électroniques, les *m-payments*.

L'usage de réseaux ouverts permet la participation d'entrepreneurs non bancaires au secteur des paiements de masse. L'observation des solutions de paiements électroniques et mobiles indique une propension à la coopération entre les nouveaux intervenants et les banques. Ces dernières se révèlent incontournables.

D'autre part, l'utilisation de réseaux ouverts soulève des craintes en matière de sécurité et de fraude. Les autorités monétaires et publiques doivent en tenir compte. Une solution consiste en l'intégration de règles spécifiques relatives aux réseaux ouverts dans les normes de surveillance applicables aux systèmes de paiement et à leurs prestataires.

La sécurité et l'efficience des systèmes et des instruments de paiement font partie intégrante des intérêts des autorités publiques et en particulier des autorités monétaires. Le SEBC a initié plusieurs consultations en matière de systèmes et d'instruments de paiement de masse. Il confirme aussi son rôle de catalyseur en collaborant avec tous les autres acteurs du marché en vue de la détermination de standards, notamment de sécurité. Une réflexion commune sur les besoins en standardisation et en interopérabilité permettront l'aboutissement d'une harmonisation en matière d'instruments de paiement électroniques.

6 Bibliographie

Publications

Banque de France, Banque de France Bulletin N° 101 - Digest, Overseeing the security of payment instruments: a greater role for the Banque de France, May 2002

Banque de France, Bulletin de la Banque de France N° 98, La sécurité des moyens de paiement sur Internet, Février 2002

Banque de France, Les moyens de paiement et les systèmes d'échange et de règlement, 1998

BCE - ECB, Blue Book Payment and securities settlement systems in the European Union, June 2001

BCE - ECB, Issues Paper: E-payments in Europe - The Eurosystem's Perspective, September 2002

BCE - ECB, Report on Electronic Money, August 1998

BCE - ECB, Monthly Bulletin November 2000, Issues arising from the emergence of electronic money

BCE - ECB, Monthly Bulletin, The role of the Eurosystem in payment and clearing systems, April 2002

BCL, Bulletin de la BCL 2001/1, Effets du développement de la monnaie électronique

Birch David, E-money and Payment Systems Review, Retail electronic payments, Central Banking Publications, 2002

Böhle Knud, ePSO Newsletter 6, Access is King: About the Bright Future of Server-based E-payment Systems, March 2001

Böhle Knud, ePSO Newsletter 8, Electronic Payments 2001 - Food for Thought, July 2001

BRI - BIS, Comité sur les systèmes de paiement et de règlement, Principes fondamentaux pour les systèmes de paiement d'importance systémique, janvier 2001

BRI - BIS, Committee on Payment and Settlement Systems, A glossary of terms used in payments and settlement systems, January 2001, revised July 2001

BRI - BIS, Basel Committee for Banking Supervision, Electronic Banking Group White Paper, Electronic Banking Risk Management Issues for Bank Supervisors, October 2000

BRI - BIS, Committee on Payment and Settlement Systems, Policy issues for central banks in retail payments, September 2002

BRI - BIS, Committee on Payment and Settlement Systems, Retail Payments in Selected Countries: A Comparative Study, September 1999

Carat Gérard, ePSO Background Paper No. 9, ePayment Systems database - Trends & Analysis - March 2002

Carat Gérard, IPTS Rapport no 49, Mobile Payments: Alternative Platforms and Players, novembre 2000

Centeno Clara, ePSO Newsletter 8, Mobile Payment Industry Fora - Consolidation of Initiatives Expected, July 2001

Combe François et Thierry Tacheex, L'essentiel de la monnaie, Gualino, 2001

Commission des Communautés européennes, Communication de la Commission au Conseil et au Parlement: Commerce électronique et services financiers, 2001

CSSF, Services financiers par Internet, décembre 2001

Dalloz, Précis d'Economie politique: la monnaie, la répartition, les échanges internationaux, 1984

European Card Review, January/February 2002

European Card Review, July/August 2001

European Card Review, July/August 2002

European Card Review, March/April 2002

Financial Times, M-commerce: Shoppers wait to ring up the till, 23 October 2002

Financial Times, Next-generation services have yet to fit the bill, 17 July 2002

Goodlet Clyde, Revue de la Banque du Canada, Les principes fondamentaux afférents aux systèmes de paiement d'importance systémique et leur application au Canada, printemps 2001

GSM Association, White Paper on Micro-Payments, July 2002

Hallsenius Johan, BrainhHeart Magazine, The Virtual Bank 2002: Operators Lead the Way but Banks will Prevail, April 2002

Henkel Joachim et Zimmermann Felix, Rapport IPTS No 63, La dimension politique des innovations dans les systèmes de paiement: le cas des paiements mobiles, avril 2002

ILReS - Plan d'action eLuxembourg 2001

Krueger Malte, ePSO Background Paper No. 2, The Future of M-payments - Business Options and Policy Issues -, August 2001

Krueger Malte, ePSO Background Paper No. 5, Innovation and Regulation - The Case of E-Money Regulation in the EU -, January 2002

Krueger Malte, ePSO Newsletter 2, M-Payments and the role of telcos, October 2000

Kuttner Kenneth N. and McAndrews James J., FRBNY Economic Policy Review, Personal On-Line Payments, December 2001

Leinonen Harry, BIS Papers No 7, Developments in retail payment systems, November 2001

Lelieveldt Simon, ePSO Newsletter 1, Where EMI-directive and mobile phone payment systems will meet ..., July 2000

Massey Kathy, E-money and Payment Systems Review, Key developments in the payments industry, Central Banking Publications, 2002

Mobey Forum, The Preferred Payment Architecture Executive Summary, Version 1.0, June 2001

Monetary Authority of Singapore, Security Guidelines for Mobile Banking & Payments - Draft, Version 1.1, 15 February 2002

Mykkänen Niko, CommerceNet Scandinavia, Mobile Payments: A report into the state of the market, October 2001

Sciusco Luigi, ePSO Newsletter 15, I-Payments Strategies, June 2002

Technology in banking and finance magazine, Issue 21, Mobile masterclass, September 2002

Van den Nieuwenhof Jozef, Euro-retail payments at crossroads?, May 2001

Sites Internet visités

- Réglementation et législation

Au Grandu-Duché de Luxembourg: www.memorial.lu
En Europe: http://europa.eu.int/eur-lex/

- Statistiques et informations sectorielles

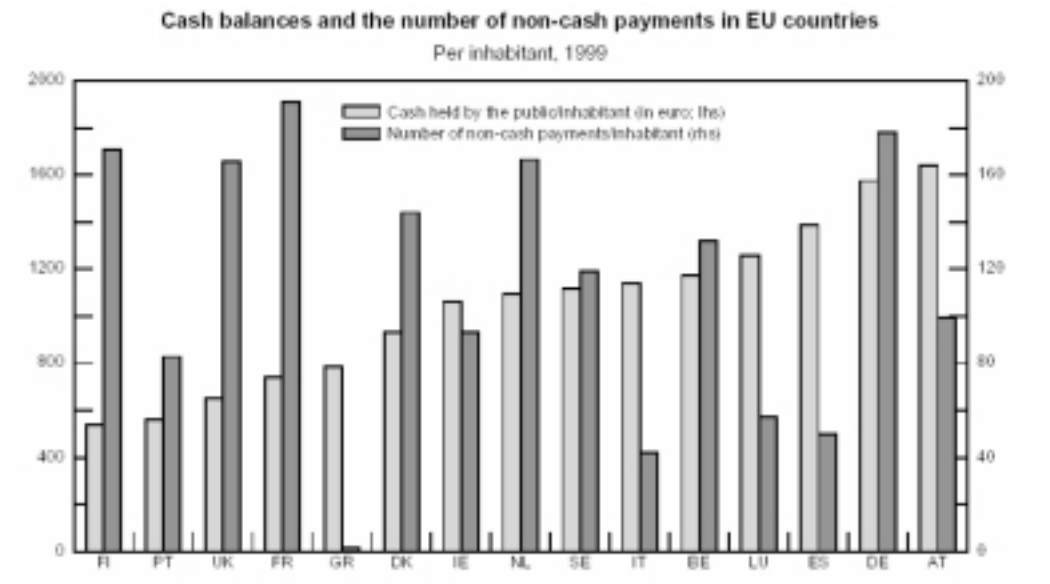
www.cellular-news.com: intentions de paiements mobiles
www.eluxembourg.lu
www.eurosmart.com: statistiques cartes à puce

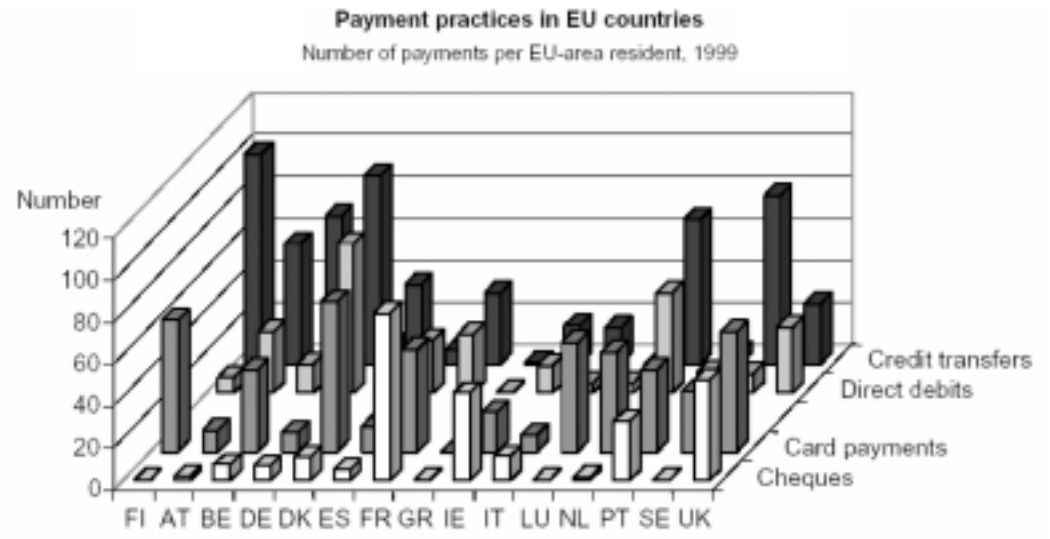
- Paiements électroniques

www.bibit.com
www.cartes-bancaires.com
www.ertico.com/telepay
www.etrasoft.be
www.mobipay.com
www.ogone.be
www.orange.fr
www.paybox.co.uk
www.paypal.com
www.postbank.nl
www.sonera.com
www.vodafone.com

Annexe 1: Statistiques instruments de paiement

Ces deux tableaux permettent de comparer l'utilisation de monnaie fiduciaire et d'instruments de paiement scripturaux au sein de l'Union européenne.





Source: BCE, cité par Leinonen Harry, BIS Papers No 7, Developments in retail payment systems

Annexe 2: Réseaux de communication sans fil

La seconde génération de téléphonie mobile

La norme de téléphonie mobile digitale GSM -*Global System for Mobile Communication*- est principalement déployée en Europe, en Afrique et en Asie-Pacifique. Les Etats-Unis connaissent une coexistence de réseaux analogiques et digitaux. Parmi ces derniers, on y retrouve des réseaux de norme GSM et CDMA -*Code Division Multiple Access*. Le CDMA est aussi mis en œuvre au Japon et en Corée du Sud.

La sécurité d'un réseau GSM se fonde sur une carte à puce, la SIM -*Subscriber Identity Module*- qui permet d'identifier l'utilisateur et, grâce à son code PIN, de l'authentifier. En outre, elle contient un algorithme servant au cryptage et au décryptage des communications transposées par ondes radio.

La carte SIM fait partie de la norme GSM. Cette carte n'est pas utilisée dans d'autres standards de téléphonie mobile tels que le CDMA dans lequel les paramètres d'identification de l'utilisateur sont intégrés dans le téléphone mobile.

Une autre distinction majeure entre les normes GSM et CDMA est le *roaming* international. De par son développement européen et pour surmonter les restrictions de mobilité des réseaux de première génération, la norme GSM avait dès le départ été pensée pour permettre à son utilisateur de passer les frontières tout en continuant à faire usage de son téléphone mobile sans formalités (une seule facture et un seul numéro d'appel où que l'on soit) grâce aux accords bilatéraux signés entre opérateurs de téléphonie mobile.

Evolution des réseaux de communication sans fil

La troisième génération de téléphonie mobile, l'UMTS -*Universal Mobile Telecommunications System*- est établie en Europe comme l'évolution du GSM. L'UMTS usera donc des mêmes modes de sécurisation, basés sur la carte SIM. D'autant plus que la mise en œuvre de l'UMTS se fera d'abord dans des zones à plus forte demande, les abonnés UMTS devront se rabattre sur un réseau GSM dans les localisations développées tardivement. Cette stratégie de déploiement nécessite des terminaux mobiles bi-modes: UMTS et GSM. Les différences techniques essentielles entre les deux technologies concernent le spectre radioélectrique et le mode de transport des données, l'Internet Protocol (IP). Pour l'utilisateur, l'avantage marquant sera un accès à haut débit permettant un accès Internet.

Le retard pris par les opérateurs dans le déploiement de l'UMTS est une opportunité pour les réseaux sans fil Wi-Fi -*Wireless Fidelity*. Leur coût de déploiement est moins élevé pour un débit théorique de 11 Mbits/s. A titre indicatif, le débit maximal de l'UMTS est de 2 Mbits/s et celui du GSM de 9,6 Kbits/s. La norme Wi-Fi est par exemple à la base des WLAN -*Wireless Local Area Network*- dédiés à un usage dans une zone géographique limitée. L'accès en est soit privé (aire de bureaux, campus...) soit public (aéroport, gare, hôtel,...). Toutefois, cette opportunité répond à des besoins nomades plutôt que mobiles car la norme Wi-Fi ne traite pas du transfert des connections d'une zone à une autre. Une autre alternative de réseau sans fil bien implantée se base sur la norme Bluetooth. Deux utilisateurs Bluetooth connectés créent un WPAN -*Wireless Personal Area Network*.

Le retard des réseaux de 3ème génération est en partie comblé par le GPRS -*General Packet Radio Service*- basé également sur le protocole IP et qui permet un accès Internet par l'intermédiaire du protocole WAP -*Wireless Application Protocol*. Le GPRS est considéré comme étant de la 2,5 génération.

Le protocole WAP est devenu un standard international dont la fonction est de formater les données échangées entre un terminal mobile et un environnement Internet. Ce protocole est adapté aux différentes technologies de réseaux de communication (GSM, GPRS, UMTS, ...)

Terminaux mobiles en tant que terminaux de paiement

Outre les considérations de modélisation de solutions de paiements mobiles, la question de l'implémentation technique se pose également. Plusieurs possibilités techniques existent pour transformer le terminal mobile en terminal de paiement.

Certaines solutions ne nécessitent aucune modification des terminaux mobiles. Principalement lorsque ces derniers servent aux micro-paiements ou uniquement à la confirmation de paiements.

Les opérateurs de solutions de paiements mobiles préfèrent garder le contrôle et opèrent les applications d'autorisation et de paiement car la possibilité de les loger dans le terminal mobile pose des problèmes de sécurité. Tous les éléments utiles seraient aux mains de potentiels fraudeurs. En outre, le client serait lié de façon plus stricte à sa banque.

L'infrastructure WIM-*Wireless Identity Module*- a été développée dans le but d'authentifier l'acheteur lors d'une transaction de paiement mobile. Comme pour les cartes de paiement, son intégration peut se faire sous différents formats:

- Carte à puce propre

Les terminaux mobiles doivent être équipés de deux lecteurs de cartes à puce (appareils bi-fentes utilisés dans la solution "CB sur mobile") ou accepter un lecteur externe de carte WIM.

Cette solution est peu pratique mais elle permet l'indépendance par rapport au fournisseur des services de paiements. Elle se complique davantage avec l'interface avec un lecteur externe.

- Puce insérée dans le téléphone

Une puce séparée contenant les applications nécessaires à l'infrastructure WIM est insérée dans le téléphone.

Cette alternative est plus pratique à mettre en œuvre et ne remet pas en cause l'indépendance du choix de paiement.

- Applications WIM intégrées dans la puce d'une carte SIM

Cette éventualité est la plus pratique tant pour les utilisateurs (au coût de leur indépendance) que les équipementiers. Mais à qui incomberaient la responsabilité et la propriété de la carte? Seuls les opérateurs ont un contrôle sur les cartes SIM, et donc les éventuelles cartes SIM-WIM, en circulation.

Annexe 3: Sécurité des réseaux de communication sans fil

La sûreté opérationnelle d'un instrument de paiement s'établit par l'application de techniques logicielles de sécurité (leur but est de garantir l'authenticité, la confidentialité et/ou l'intégrité de la transaction) sur un support physique de sécurité. Une combinaison est nécessaire pour atteindre un niveau de sécurité déterminé dans la politique de sécurité choisie. Par exemple, il sera préférable de sauvegarder un logiciel sécuritaire sur une carte à puce plutôt que sur un disque dur d'ordinateur qui est facilement copiable ou exportable.

Support physique

Le support physique permet de limiter l'accès au réseau ouvert. Pour les réseaux sans fil, nous pouvons prendre deux exemples.

- La carte à puce

Dans le domaine des paiements, la carte à puce est utilisée pour le porte-monnaie électronique, l'accès à l'*e-banking*, les cartes de crédit…

La puce est intéressante par ses capacités de mémoire et de calcul grâce à la présence d'un microprocesseur. Ce dernier peut servir au traitement de plusieurs types d'applications au sein d'une même puce (carte multi-applications) parmi lesquelles des applications de sécurité. La sécurité est en effet une caractéristique importante de la carte à puce par rapport aux cartes à bande magnétique: la puce est difficile à falsifier, elle est protégée par un code PIN, elle est capable d'exécuter du cryptage et elle est identifiée par un numéro de série unique.

D'autre part, de par sa taille et de par son intégration dans un terminal mobile de communication, la puce est hautement mobile et présente l'avantage de pouvoir être mise à jour sans devoir émettre une nouvelle puce. Le développement de carte à puce sans contact -*contactless smart card*- augmente encore la mobilité et la facilité d'utilisation.

- Le spectre radioélectrique

Un réseau de communication sans fil est notamment caractérisé par son spectre radioélectrique (sa fréquence d'accès). Par exemple, la norme GSM initiale est dite de fréquence de 900 MHz. En fait, les communications sont établies sur une fréquence allouée par le réseau à chaque communication dans la gamme de 875 MHz à 915 MHz. Cette contrainte physique permet déjà une première restriction d'accès au réseau. Ensuite d'autres applications sécurisées de transmissions sont mises en place: modulation, encodage, cryptage…

Techniques logicielles

Garantie de l'authenticité des parties

Ces techniques visent à s'assurer de l'identité et de l'authenticité des parties qui communiquent lors d'une transaction.

- Le mot de passe à usage unique

L'utilisateur qui désire s'authentifier utilise son code PIN et l'algorithme qu'il a reçu préalablement pour obtenir un mot de passe à usage unique. Le code est généré en fonction de la date et de l'heure, ce qui garantit son unicité.

- La technique du défi-réponse (*challenge*)

L'utilisateur A qui cherche à s'authentifier auprès de B l'en informe. B envoie à A un nombre aléatoire (le défi) que A combine avec un secret pour générer le résultat (la réponse) qui est alors envoyé à B. B vérifie la réponse qu'il reçoit avec le résultat qu'il a lui-même calculé. Si les résultats concordent, l'authentification est réussie.

Le secret utilisé ici peut être une clé symétrique (partagée par A et B pour le calcul de la réponse et de sa vérification) ou une clé asymétrique (la clé servant au calcul de la réponse est différente de celle utilisée pour la vérification). Plus de détails sont expliqués dans le paragraphe suivant.

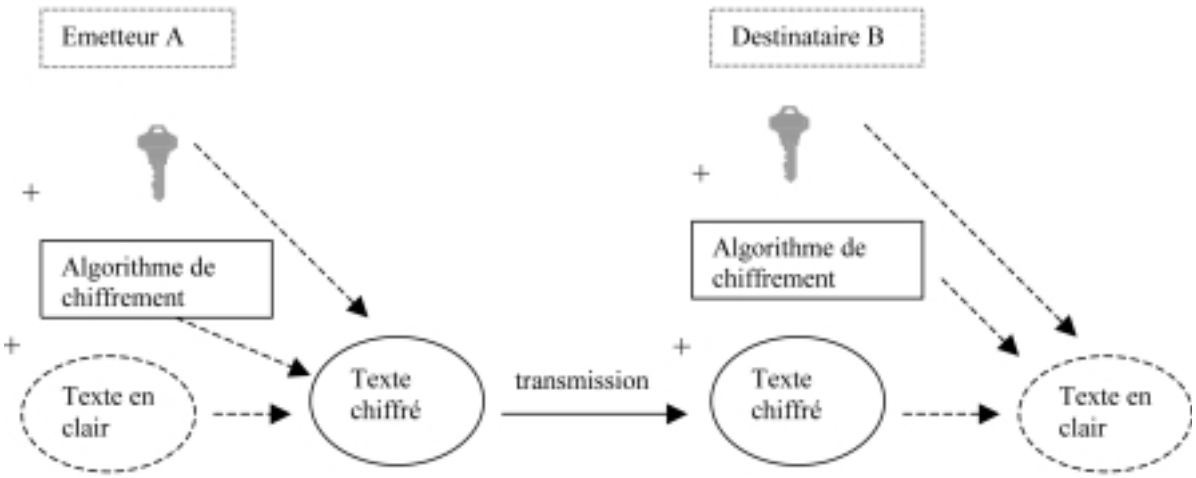
Garantie de l'intégrité et/ou de confidentialité

A la différence des techniques décrites dans le paragraphe précédent, les systèmes expliqués ici ont pour but de garantir l'intégrité et/ou la confidentialité en sus de l'authenticité. Ces systèmes sont classés entre systèmes symétriques et asymétriques.

- Les systèmes symétriques

Les parties A et B (émetteur et destinataire) partagent la même clé (ou secret) qui sert au chiffrement et au déchiffrement du message échangé. La clé permet d'authentifier les correspondants, mais aussi d'assurer la confidentialité et l'intégrité de la transmission.

Figure 1 - Système symétrique de cryptage



Nécessitant simplement des accords bilatéraux, un tel système est assez facile à déployer. Il requiert néanmoins l'obligation de devoir échanger une clé avec chaque partenaire de transmission, par un canal séparé.

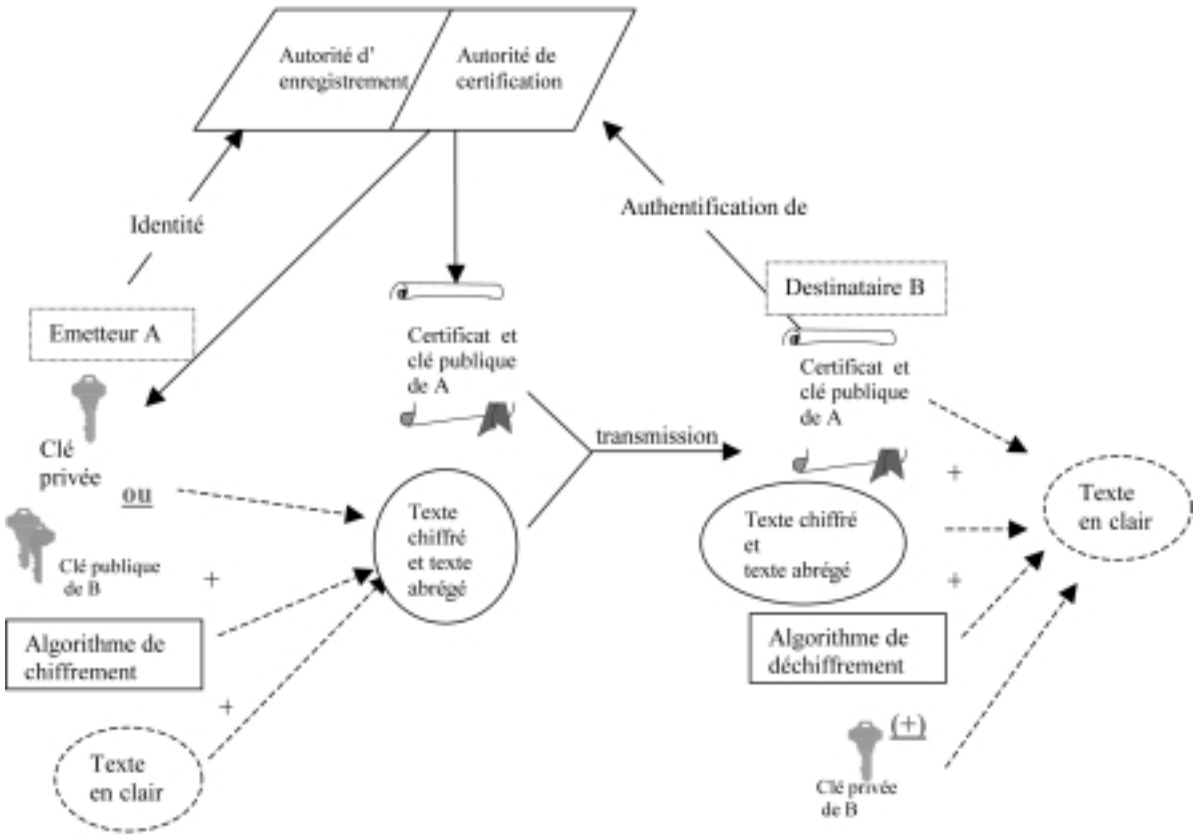
- Les systèmes asymétriques

L'émetteur (A) utilise sa clé privée pour chiffrer le message et le signer. A envoie le message et son certificat numérique au(x) destinataire(s). A s'est au préalable inscrit auprès d'une autorité d'enregistrement et de certification qui lui a délivré un certificat numérique (qui contient sa clé publique et qui établit son identité). Le(s) destinataire(s) **authentifient** l'émetteur grâce au certificat numérique de A, en vérifiant sa validité au moyen de la clé publique de l'autorité de certification. La clé publique de A servira au déchiffrement du message, ce qui permettra d'en garantir **l'intégrité** en comparant le message décrypté et le message abrégé. Dans cette alternative, A ne cherche pas à assurer la confidentialité de son message.

Si A veut être sûr que seul le destinataire B pourra déchiffrer son message (**confidentialité**), A devra chiffrer le message en utilisant la clé publique de B et signer avec sa propre clé privée. De cette façon, B pourra **authentifier** A grâce au certificat numérique de A qui accompagne le message. Seule la clé privée de B permet de déchiffrer le message crypté par la clé publique de B.

Un tel système de cryptographie basé sur une clé publique et une clé privée est appelé PKC - *Public Key Cryptography*. Lorsque le système inclut une tierce partie qui émet les certificats numériques, il est appelé infrastructure à clé publique ou PKI -*Public Key Infrastructure*.

Figure 2 - système asymétrique de chiffrement



Cette infrastructure PKI est beaucoup plus complexe à mettre en œuvre, surtout en ce qui concerne l'établissement des autorités d'enregistrement et des autorités de certification: leur reconnaissance internationale, leur interopérabilité et la procédure d'enregistrement qui garantit la véritable authentification du demandeur du certificat numérique.

- Secure Socket Layer

Le protocole SSL -*Secure Socket Layer*- assure la confidentialité et l'intégrité des messages transmis sur Internet. Il est aussi utilisé pour sécuriser les paiements sur Internet. Les porte-monnaie électroniques répondant aux spécifications CEPS -*Common Electronic Purse Specifications*- utilisent le PKC pour l'authentification mutuelle entre la carte et le marchand.

- Secure Electronic Transaction

Le protocole de paiement sécurisé SET -*Secure Electronic Transaction*- utilise le PKC, les certificats numériques et la signature digitale pour assurer l'authentification, la confidentialité, l'intégrité et la non répudiation de la transaction. Ce protocole implique l'intervention d'une autorité de certification.

- PKI sans fil

WPKI -*Wireless PKI*- se définit comme une application PKI lorsque la communication entre l'appareil du consommateur et une tierce partie se fait sans fil. L'application peut être logée dans une carte à puce, la carte WIM, l'équivalent de la carte SIM pour l'identification d'une personne, lors d'un paiement par exemple. Se basant sur la technologie PKI, elle permet une identification plus forte de l'acheteur car elle incorpore un certificat digital autorisant l'acheteur à signer électroniquement. Un des buts recherchés ainsi est de transformer un terminal mobile en appareil de paiement.

Plusieurs solutions ont déjà été déployées (Sonera avec Europay International, Orange France avec le Groupement des Cartes Bancaires....) avec comme seul trait commun l'utilisation d'une carte à puce comme support de la clé privée et du certificat numérique. L'identification est décidée par l'émetteur de la carte de paiement, les logiciels de sécurité peuvent être sauvegardés sur la même carte SIM, sur la puce de la carte de paiement (carte à double puce nécessitant un téléphone à deux lecteurs) ou sur une autre puce de la carte SIM (téléphone bi-fente). La pléthore de solutions met en évidence l'intérêt que le marché porte sur la sécurité des transactions mobiles. Mais le manque de standardisation peut freiner son développement.