M0074 MBF05

CESAG

BCEAO

IBF

3ème Cycle / **MASTERE EN BANQUE ET FINANCE**

SECURISATION DES MOYENS DE PAIEMENT SCRIPTURAUX DANS LES PAYS DE L'UEMOA

MEMOIRE DE FIN D'ETUDE

POUR L'OBTENTION DU MASTER EN BANQUE ET FINANCE

OPTION : BANQUE ET MAITRISE DES RISQUES

PRESENTE PAR : **Mahamane Laouali SANI**

DIRECTEUR DE MEMOIRE : **Bwaki KWASSI**
SOUS-DIRECTEUR
Direction des Systèmes de Paiement
BCEAO-Siège

M0074MBF05

2

UE 2003-2004

Bibliothèque du CESAG
107856

CESAG BIBLIOTHEQUE

SOMMAIRE

RESUME P1

SUMMARY P5

INTRODUCTION P8

PREMIERE PARTIE : CADRE THEORIQUE ET METHODOLOGIQUE

I- CADRE THEORIQUE P10

I-1- PROBLEMATIQUE P10

I- 2- OBJECTIFS P10

I-3- HYPOTHESES P11

I-4- PERTINENCE DU SUJET P11

II- CADRE METHODOLOGIQUE P11

DEUXIEME PARTIE : SITUATION DES MOYENS DE PAIEMENT DANS LA ZONE EURO

I- ANALYSE DE LA SITUATION DES MOYENS DE PAIEMENT P12

I-1- SECURITE DES CHEQUES P15

I-2- SECURITE DES VIREMENTS ET PRELEVEMENTS P15

I-3- SECURITE DES CARTES BANCAIRES P16

I-4- SECURITE DES PAIEMENTS EN LIGNE P16

II- CADRE JURIDIQUE ET LEGAL P17

TROIXIEME PARTIE : SITUATION DES INSTRUMENTS DE PAIEMENT SCRIPTURAUX DANS L'UEMOA

I- ETAT DES LIEUX P18

I-1- LE CHEQUE P18

I-2- LE VIREMENT P20

I-3- LES EFFETS DE COMMERCE P20

I-4- LA CARTE BANCAIRE P22

CESAG BIBLIOTHEQUE

II- GESTION DES RISQUES **P24**

II-1- LA CARTE BANCAIRE P24

II-2- LE CHEQUE P26

III- SECURISATION DES MOYENS DE PAIEMENT SCRIPTUAUX **P26**

III-1- SECURISATION TECHNIQUE P26

III-1-1- LA CARTE BANCAIRE P26

III-1-2- LE CHEQUE P30

III-2- SECURISATION JURIDIQUE P33

IV- QUEL CADRE REGLEMENTAIRE ET PRUDENTIEL POUR L'EMISSION DE LA MONNAIE ELECTRONIQUE ? **P36**

IV-1- RISQUES LIES A L'EMISSION DE LA MONNAIE ELECTRONIQUE P37

IV-1-1- RISQUE OPERATIONEL P37

IV-1-2- RISQUE JURIDIQUE P37

IV-1-3- RISQUE D'UTILISATION CRIMINELLE P38

IV-1-4- RISQUE DE REPUTATION ET DE CONFIANCE P38

IV-1-5- RISQUE DE DEFAILLANCE P38

IV-2- PROPOSITION DE DISPOSITIF REGLEMENTAIRE ET PRUDETIEL P40

CONLUSION **P43**

GLOSSAIRE P44

ANNEXES P51

GRAPHIQUE 1 : FRANCE : OPERATIONS ECHANGEES DANS LE SYSTEME BANCAIRE EN 2003 P13

GRAPHIQUE 2 : ZONE EURO : OPERATIONS ECHANGEES EN 2003 P13

GRAPHIQUE 3 : REPARTITION DES MOYENS DE PAIEMENT SCRIPTURAUX DANS L'UE EN % DE VOLUME : EVOLUTION 1996-2001 P14

GRAPHIQUE 4 : NOMBRE ANNUEL DE TRANSACTIONS SCRIPTURALES PAR HABITANTS EN 2001 P14

TABLEAU1 : REPARTITION DES ETABLISSEMENTS DE CREDIT PAR PAYS P18

CESAG - BIBLIOTHEQUE

DEDICACES

Je dédie le fruit de ce travail à mes parents, pour tous les sacrifices qu'ils ont consenti afin de faire de moi un homme responsable, bien éduqué et formé. Aussi, je voudrais les remercier pour tout le soutien et l'aide qu'ils m'ont accordés dans les moments les plus difficiles. Je vous remercie pour tout, et que Dieu vous bénisse et vous donne longue vie.

Je fais un clin d'œil à toute ma famille ainsi qu'à ma fiancée pour leurs précieux conseils. A tous, je dis merci !

CESAG - BIBLIOTHEQUE

REMERCIEMENTS

Je tiens à remercier Monsieur Charles Konan BANNY, **GOUVERNEUR** de la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) d'avoir permis ce stage en m'accueillant dans son Institution ainsi que Madame Fatimatou Zahra DIOP, **DIRECTEUR** des Systèmes de Paiement, Monsieur SEREME, **DIRECTEUR-ADJOINT** des Systèmes de Paiement, sans oublier mon **Maître de stage et Directeur de mémoire**, Monsieur Bwaki KWASSI qui n'a ménagé aucun effort pour m'aider pendant ce stage.

Je souhaite également faire part de ma reconnaissance à tous les Responsables de volet, Mesdames et Messieurs Akuwa AZOMA, **Responsable SICA**, Bourry DIALLO, **Responsable Comptable et Financier**, Pape Mbaye DIEYE, **Responsable Monétique**, A.ALTINE, **Responsable du Cadre Réglementaire et Légal**, pour leur assistance précieuse durant ces trois mois ainsi qu'à l'ensemble du personnel qui m'a aidé dans mes recherches pendant mon stage et qui a contribué à créer les conditions de travail exemplaires.

Mes remerciements s'adressent également à Monsieur Roger ATHINDEHOU, **Chef de Projet du Master en Banque et Finance** au CESAG, ainsi qu'à tous les professeurs qui ont contribué à ma formation.

CESAG - BIBLIOTHEQUE

RESUME

Dans les pays de l'UEMOA, un grand nombre de règlements s'effectue en espèces. D'où la prédominance de la monnaie fiduciaire sur les moyens de paiement scripturaux tels que le chèque, la carte bancaire, le prélèvement automatique et le virement bancaire.

Le taux de bancarisation est inférieur à 10%, soit parmi les plus faibles au monde. Cette situation a été surtout favorisée par la suprématie du secteur informel, le manque de confiance dans le système bancaire, la vétusté des systèmes de paiement. Face à tous ces dangers grandissants et menaçants, la BCEAO a entrepris avec l'aide des partenaires étrangers, de réformer ses systèmes et moyens de paiement pour répondre non seulement aux besoins des populations en quête permanente de sécurité et de fiabilité des instruments de paiement, mais aussi pour répondre aux normes internationales, par le renforcement des infrastructures de base du secteur financier, la réduction des coûts et des délais de traitement des opérations de paiement, l'amélioration de la sécurité des opérations et la promotion de nouveaux instruments de paiement électronique.

Pour assurer un niveau de sécurité des instruments de paiement à la hauteur de ces enjeux, les entreprises bancaires doivent investir dans les technologies reconnues de plus en plus efficaces (cartes à puce, cryptologie, Echange d'Images Scannées…).

SITUATION DES MOYENS DE PAIEMENT ET RECOMMANDATIONS

Au 28 juillet 2004, le nombre de banques agréées par les autorités monétaires était de 74 contre 24 pour les établissements financiers. Les moyens de paiement scripturaux les plus usités sont le chèque, le virement, les effets de commerce, la carte bancaire et les prélèvements automatiques.

- Le chèque constitue le moyen de paiement le plus utilisé dans les transactions économiques. Il représente en moyenne 85% du volume et 62% de la valeur des paiements scripturaux. Le chèque se caractérise par son graphisme, les encres utilisées (leur couleur, leur intensité et leur sensibilité éventuelle) ainsi que le papier utilisé et sa sensibilité éventuelle. Il en est de même pour le choix du graphisme, du procédé d'impression, sans oublier les techniques et précautions qui pourront dissuader les fraudeurs.

  Du fait de son support papier, et les informations non cryptées, le chèque comporte des faiblesses en terme de sécurisation. L'Echange Image Scannée (EIS) a été mis en place pour dématérialiser le traitement des chèques. En diminuant fortement la circulation et les manipulations des vignettes (chèques), il permet de limiter les risques de fraude.

CESAG - BIBLIOTHEQUE

- La carte bancaire est très peu utilisée dans les pays de l'UEMOA. Peu de fraudes sont constatées jusque là, mais de nombreux risques subsistent. Seules les cartes privatives à usage de retrait ont fait l'objet de fraudes de faible envergure. Par contre les fraudes sur les paiements sont beaucoup plus importantes sur les cartes internationales et se présentent essentiellement sous forme de contrefaçon.

  Face à toutes ces insuffisances sécuritaires de cette ampleur, il est impératif pour le système bancaire de l'UEMOA, de renforcer la sécurité de ses cartes bancaires, en adoptant les nouvelles générations de cartes à puce respectant la norme Europay MasterCard Visa en remplacement des cartes à piste magnétique actuellement usitées dans les pays l'Union.

  Une autre recommandation faite pour la sécurisation des cartes bancaires, est la biométrie associée au système interbancaire de paiement par cartes.

  La biométrie est la science qui permet d'identifier automatiquement un individu en se basant sur ses caractéristiques physiologiques ou comportementales. Généralement, on distingue deux catégories de méthodes d'authentification biométrique : les méthodes basées sur les caractéristiques physiques (visage, voix, iris, rétine, pouce, forme de la main et de l'oreille, ADN, système veineux) et celles basées sur les caractéristiques comportementales comme la signature, la manière de marcher ou de taper sur un clavier *(keystroke dynamics)*.

  Ainsi, à partir du processus d'identification traditionnellement utilisé par les forces de police ainsi que les services d'immigration, nous proposons la procédure suivante pour les transactions par cartes bancaires :

- lors de la personnalisation de la carte bancaire par le concepteur, des caractéristiques physiques uniques de l'individu (visage, voix, iris, rétine, pouce, forme de la main), doivent être intégrées sur la puce de la carte ;

- Les terminaux de paiement sont équipés de capteurs utilisés pour acquérir une caractéristique spécifique de l'utilisateur et capables d'identifier l'émetteur de la transaction, en confrontant les caractéristiques physiques scannées de la personne, à celles déjà stockées sur la puce électronique ;

- S'il y a compatibilité, le terminal continue les autres procédures de vérification.

CESAG BIBLIOTHEQUE

- S'agissant du virement, sa part relative dans les paiements scripturaux est de 13% en terme de volume et 29% en valeur. Il est surtout utilisé par les entreprises pour le paiement des salaires et les nivellements des comptes entre le siège et les succursales.
  Cet instrument de paiement dématérialisé, doit être construit de telle sorte que les règles contractuelles banques/clients assure une très forte sécurité pour le client.
  Ainsi, les banques doivent mettre en place des dispositifs afin de vérifier l'identité du donneur d'ordre et son habilitation à faire un virement sur le compte destinataire. Il s'agit d'éviter toute usurpation de coordonnées bancaires en amont, lors de l'envoi d'un ordre de virement, et en aval de s'assurer qu'il n'y a pas de détournement de fonds.

- Le prélèvement automatique est d'utilisation plus récente, mais fortement recommandé par les grandes entreprises, telles que les compagnies d'eau, d'électricité et de téléphone. L'entreprise bénéficiaire propose cette formule de paiement uniquement à ses clients possédant un compte bancaire auprès d'un établissement de crédit. Les montants des prélèvements ne sont imputés au compte du débiteur que quelques jours plus tard.
  Le prélèvement est soumis dans l'UEMOA à des règles professionnelles très strictes, afin de lui assurer un taux de fraude minime. Les créanciers destinataires des prélèvements sont par exemple identifiés et enregistrés auprès de la BCEAO.

- Les effets de commerce sont faiblement représentés dans les transactions économiques et sont souvent utilisés comme instruments de crédit.
  Ils sont concernés par les mêmes normes de sécurité que les chèques.

Le nouveau dispositif légal et réglementaire vise donc à garantir la sécurité des messages qui seront transmis. Il permet, d'une part, de prendre en considération les nouveaux instruments électroniques de paiement et d'autre part, de tirer les conséquences, au plan de la politique criminelle, de cette nouveauté, en prévoyant un traitement approprié des infractions pouvant naître de l'utilisation des nouveaux instruments de transfert électronique de fonds.
Ainsi, en ce qui concerne le chèque, la principale innovation consiste dans la mise en place d'un fichier central des incidents de paiement, au niveau de l'UEMOA, dont la gestion est confiée à la BCEAO. Les informations étant fournies par chaque banque ou établissement financier dans le but de centraliser tous les incidents de paiement, de responsabiliser et sensibiliser les établissements de crédit sur les risques potentiels dont elles peuvent être

CESAG - BIBLIOTHEQUE

victimes, d'accélérer les échanges d'informations entre les établissements de crédit et la BCEAO.

Les incidents de paiement relatifs à la lettre de change et au billet à ordre obéissent aux mêmes règles.

En ce qui concerne les cartes, la loi distingue la carte de retrait et la carte de paiement. Elle a encouragé la création d'un Groupement Interbancaire Monétique chargé d'instituer et de gérer des cartes transnationales. Le GIM-UEMOA assure les fonctions dites de gouvernance telles que l'organisation de l'interbancarité, l'élaboration des règles et procédures interbancaires et la gestion de la fraude.

S'agissant du règlement des paiements électroniques, Le problème essentiel en matière de paiements électroniques est double : quand est ce qu'un paiement est considéré comme irrévocable ? Et comment prouver de manière estimée irréfutable par la loi que l'ordre de paiement a bien été effectué et émanait bien de celui qui prétend l'avoir effectué.

Le besoin d'instaurer une réglementation prudentielle a été motivé par l'existence de plusieurs types de risques potentiels parmi lesquels: le risque que le système ne fonctionne pas comme prévu pour des raisons opérationnelles ou techniques ; le risque juridique inhérent à une définition floue des droits et obligations en vertu de la loi ; le risque d'utilisation du système à des fins criminelles, y compris la fraude, entraînant des pertes de taille pour les promoteurs du système ; le risque de réputation et de confiance.

CESAG - BIBLIOTHEQUE

RESUME

Dans les pays de l'UEMOA, un grand nombre de règlements s'effectue en espèces. D'où la prédominance de la monnaie fiduciaire sur les moyens de paiement scripturaux tels que le chèque, la carte bancaire, le prélèvement automatique et le virement bancaire.

Le taux de bancarisation est inférieur à 10%, soit parmi les plus faibles au monde. Cette situation a été surtout favorisée par la suprématie du secteur informel, le manque de confiance dans le système bancaire, la vétusté des systèmes de paiement. Face à tous ces dangers grandissants et menaçants, la BCEAO a entrepris avec l'aide des partenaires étrangers, de réformer ses systèmes et moyens de paiement pour répondre non seulement aux besoins des populations en quête permanente de sécurité et de fiabilité des instruments de paiement, mais aussi pour répondre aux normes internationales, par le renforcement des infrastructures de base du secteur financier, la réduction des coûts et des délais de traitement des opérations de paiement, l'amélioration de la sécurité des opérations et la promotion de nouveaux instruments de paiement électronique.

Pour assurer un niveau de sécurité des instruments de paiement à la hauteur de ces enjeux, les entreprises bancaires doivent investir dans les technologies reconnues de plus en plus efficaces (cartes à puce, cryptologie, Echange d'Images Scannées…).

SITUATION DES MOYENS DE PAIEMENT ET RECOMMANDATIONS

Au 28 juillet 2004, le nombre de banques agréées par les autorités monétaires était de 74 contre 24 pour les établissements financiers. Les moyens de paiement scripturaux les plus usités sont le chèque, le virement, les effets de commerce, la carte bancaire et les prélèvements automatiques.

- Le chèque constitue le moyen de paiement le plus utilisé dans les transactions économiques. Il représente en moyenne 85% du volume et 62% de la valeur des paiements scripturaux. Le chèque se caractérise par son graphisme, les encres utilisées (leur couleur, leur intensité et leur sensibilité éventuelle) ainsi que le papier utilisé et sa sensibilité éventuelle. Il en est de même pour le choix du graphisme, du procédé d'impression, sans oublier les techniques et précautions qui pourront dissuader les fraudeurs.

  Du fait de son support papier, et les informations non cryptées, le chèque comporte des faiblesses en terme de sécurisation. L'Echange Image Scannée (EIS) a été mis en place pour dématérialiser le traitement des chèques. En diminuant fortement la circulation et les manipulations des vignettes (chèques), il permet de limiter les risques de fraude.

CESAG - BIBLIOTHEQUE

their clients with banking facilities. They are submitted in UEMOA zone to very restricted professional rules, so that to assure a minimum fraud rate. Beneficiary corporates of automatic deductions are for example identified and registered to BCEAO.

Banking transfers represent only 13% of the volume and 29% of the value of scriptural payments. They are used above all by corporates for payments of salaries. Banks should settle set of measures in order to verify the identity of the transaction's initiator and his ability to make transfer to someone.

- Cheque constitutes the most used instruments of payment in the economic transactions. It accounts for 85% of the volume and 62% of the value of scriptural payments. For safety measures, Due to its aspect and to its non crypted informations, the cheque comprises weaknesses in term of security. By decreasing strongly the circulation and handling of labels, that makes it possible to limit risks of fraud.

  By the same time, the banking sector is still working harder with partners, to enhance its physical security by focussing on standards on the obligatory form and mentions, graphics, ink and paper used as well as their possible sensitivity. It's the same for the choice of graphics, the impression process, without forgetting techniques and precautions, which will be able to dissuade smugglers.

- Commercial papers are weakly represented in economic transactions and are often used as instruments of credit. They are concerned by the same security norms as cheques.

The new framework aim to guaranty the security of messages transmissions. It allows, on one side, to take into account new electronic instruments of payment, and on the other side to forecast the right treatment for infractions issued from the using of new instruments for electronic transfers.

With regard to cheques, the main innovation consists in the creation of a central file for payment incidents, managed by the Central Bank. Each bank or financial institution is in the obligation to provide any information concerning payment incidents. The law allows the incident's author to put in order himself, subject to pay the amount of cheque and penalty for late, without any prejudice of penal sanctions.

With regard to banker's cards, the legal authorities have encouraged the creation of an institution (GIM-UEMOA), in charge of managing international cards and interbank transactions.

CESAG - BIBLIOTHEQUE

Regarding to electronic payments, there are two principal problems: the irrevocability of the payment and the proof that the order of payment have been given by the right person.

The need to settle a prudential regulation has been motivated by the existence of several types of potential risks like the operational and technical risk; the legal risk; the risk of using the system for criminal aims and then the risk of reputation and trust.

CESAG - BIBLIOTHEQUE

INTRODUCTION

Les systèmes économiques et financiers modernes se caractérisent par le recours aux banques et l'utilisation de moyens de paiement scripturaux que sont généralement les chèques, les virements, les cartes bancaires, les effets de commerce.

Dans les pays de l'UEMOA, la tendance est à la thésaurisation, un grand nombre de paiements se règle en espèces, l'utilisation des instruments de paiement scripturaux dans les transactions financières est faible. Il en résulte des risques liés à l'insécurité des systèmes et moyens de paiement utilisés, des lourdeurs dans les procédures de paiement et la longueur des délais de dénouement des opérations, un faible circulation de la monnaie. Ces facteurs constituent un obstacle non négligeable à l'émergence des économies des Etats de l'UEMOA. C'est pour pallier ces insuffisances que la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a initié une vaste réforme des systèmes et moyens de paiement dans les pays de l'UEMOA, en vue d'accroître le taux de bancarisation, de promouvoir l'interbancarité, de sécuriser les paiements, d'automatiser les échanges et réduire les coûts et les délais des transactions financières.

Ailleurs, les nouvelles technologies ont révolutionné l'univers de la communication permettant d'optimiser la stratégie de mondialisation. Ainsi, M. Xavier Dalloz décrit l'arrivée du «cybercommerce» dans son livre intitulé «e-business»[1] de la manière suivante «sous nos yeux, un nouveau monde est en train d'émerger. C'est un monde virtuel, c'est le 6ème continent». Les perspectives de développement du commerce électronique ont suscité, ces dernières années, une augmentation de l'offre de solutions de paiement dans ce domaine (Digicash, Protocole 3D Secure, etc…). La qualité et la sécurité de ces procédés nouveaux suscitent aujourd'hui des interrogations compréhensibles de la part de beaucoup d'utilisateurs.

La sécurité des moyens de paiement scripturaux dépend aujourd'hui fortement de leur environnement informatique. Il est par conséquent essentiel que, tout en étant économiquement viables, les moyens de paiement bénéficient d'un niveau de sécurité technique et juridique le plus élevé possible : c'est une condition nécessaire pour réduire les risques de fraude et créer les conditions d'une relation de confiance.

Notre étude intitulée « la sécurisation des moyens de paiement scripturaux en zone UEMOA », aura pour but de recenser dans un premier temps les moyens de paiement utilisés actuellement dans les pays de l'union, leur niveau de sécurité, les faiblesses et les risques de

[1] Net Economie et E-Business ; Réinventez votre système d'information autour d'Internet ;

CESAG - BIBLIOTHEQUE

fraude dont ils font l'objet, puis dans un second temps, de faire des recommandations au plan sécuritaire pour rendre les instruments de paiement scripturaux plus fiables. Cette étude portant uniquement sur les moyens de paiement scripturaux mis à la disposition des consommateurs par les établissements bancaires et financiers agréés par la Commission Bancaire, régis par la Loi Bancaire et oeuvrant dans la zone UEMOA, se déroule en trois étapes :

- La première partie, constituée de deux volets, présente les aspects théoriques et méthodologiques de l'étude ;

- La deuxième partie déclinée en deux axes, nous fournit une analyse sur la situation des moyens de paiement utilisés à travers la zone euro, notamment en ce qui concerne leur aspect sécuritaire ainsi que leur cadre juridique et légal ;

- Enfin, la troisième partie divisée quatre volets, dresse la situation des instruments de paiement dans les pays de l'UEMOA, notamment en ce qui concerne la gestion des risques potentiels dont ils font l'objet, la sécurisation de ces derniers sur le plan technique et juridique ainsi que l'élaboration d'un cadre réglementaire et prudentiel pour l'émission de la monnaie électronique.

CESAG - BIBLIOTHEQUE

PREMIERE PARTIE

CADRE THEORIQUE ET METHODOLOGIQUE

CESAG - BIBLIOTHEQUE

I- CADRE THEORIQUE

I-1- PROBLEMATIQUE

Dans un contexte de révolution des systèmes et moyens de paiement à travers le monde, l'Afrique ne peut que se mettre au pas en se dotant de nouveaux systèmes «high tech», pour lui permettre de sortir du rang des grands oubliés de la planète.

Cependant, face à une recrudescence des fraudes et de contrefaçons en milieu bancaire, ainsi qu'une mondialisation de l'économie de plus en plus pressante, la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO), a décidé d'utiliser les grands moyens pour réformer son environnement bancaire afin de pallier cette contre-performance économique et financière, occasionnée par la vétusté de ses systèmes et moyens de paiement scripturaux. Les grandes questions que l'on se pose sont les suivantes :

- Est ce que les nouveaux moyens de paiement bénéficient d'un niveau de sécurité technique et juridique le plus élevé possible et adéquat, pour ainsi réduire les risques de fraude et créer les conditions d'une relation de confiance, malgré des technologies de plus en plus complexes et variées ?

- Est-ce qu'un modèle de sécurité inspiré du modèle européen réussirait à contrer la montée en puissance de la délinquance financière ?

Face à toutes ces préoccupations, une solution s'impose : la sécurisation technique et juridique des moyens de paiement scripturaux.

Pour assurer un niveau de sécurité des instruments de paiement à la hauteur de ces enjeux, les entreprises bancaires doivent investir dans les technologies reconnues de plus en plus efficaces (cartes à puce, cryptologie, Echange d'Images Scannées…).

I- 2- OBJECTIFS

Notre étude, axée sur la sécurisation des moyens de paiement scripturaux dans la zone UEMOA, aura pour objectif de recenser dans un premier temps les moyens de paiement mis en place par la BCEAO et actuellement utilisés dans l'UEMOA, leur niveau de sécurité, les faiblesses et les risques de fraudes dont ils font l'objet. Puis dans un second temps, proposer une politique de sécurité susceptible de les rendre plus fiables, afin de contrer l'expansion des actes délictueux commis au moyen de ces derniers.

CESAG - BIBLIOTHEQUE

I- 3- HYPOTHESES

Comme hypothèses de travail, nous en avons retenu deux :

- une réforme des instruments de paiement basée sur des technologies « cartes à microprocesseur, chèques et effets de commerce dématérialisés, biométrie », ainsi que l'élaboration d'un cadre juridique et légal bien adapté à ces derniers, afin de définir les responsabilités de chaque intervenant, rendraient leur utilisation plus fiable.

- L'adoption d'une politique sécuritaire commue efficace par les pays de l'UEMOA, calquée sur le modèle européen qui est basé sur des expériences de fonctionnement de ces nouveaux moyens de paiement, permettrait d'anticiper et de se préparer contre les différents types de fraudes qui sévissent ailleurs dans le monde.

I- 4- PERTINENCE DU SUJET

Outre l'aspect très instructif du sujet, il n'en demeure pas moins qu'il planche sur un thème d'actualité. Par ailleurs, il a aussi retenu notre plus grande attention, parce qu'une réflexion est en cours sur le sujet, surtout avec le développement grandissant du système bancaire des pays de l'UEMOA. Ainsi, il présente un double intérêt :

- d'une part, pour le système bancaire, qui a comme souci premier de mettre à la disposition de sa clientèle, des moyens de paiement peu coûteux, fiables et rapides ;

- d'autre part, pour la clientèle, qui est en quête de sécurité permanente dans ses transactions financières courantes avec d'autres agents économiques.

II- CADRE METHODOLOGIQUE

Dans les pays de l'UEMOA, l'utilisation des instruments de paiement scripturaux dans les transactions financières est faible au profit de la monnaie fiduciaire. Il en résulte des risques liés à l'insécurité des systèmes et moyens de paiement utilisés, des lourdeurs dans les procédures de paiement et les délais des opérations, une faible circulation de la monnaie.

Ainsi pour apporter une solution à ce problème, la BCEAO a entrepris la réforme des systèmes et moyens de paiement. Le nouveau dispositif se met progressivement en place.

S'inscrivant dans le même sillage, le présent travail cherche à contribuer au renforcement de la sécurité des moyens de paiement au sein de l'UEMOA. Et la tâche est d'autant plus difficile que la mise en œuvre de ces nouveaux moyens de paiement est à ces débuts.

CESAG - BIBLIOTHEQUE

En fait, ce travail se veut comme étant une proposition de renforcement du dispositif sécuritaire des moyens de paiement usités au sein de l'UEMOA, inspirée du modèle de sécurité mise en place au sein de la zone euro.

Pour mener à bien notre étude et mieux répondre à nos préoccupations, nous avons effectué des recherches auprès de différentes sources : sites Internet, revues spécialisées, ouvrages traitant de la question auprès de la Banque Centrale des Etats de l'Afrique de l'Ouest, notamment au travers des publications, rapports et études de la Direction des systèmes de Paiement (DSP). Néanmoins, aucune étude statistique sur le recensement des fraudes concernant les moyens de paiement scripturaux n'a encore été faite jusqu'ici par les autorités monétaires, ce qui explique l'absence de données chiffrées pour mieux apprécier ce phénomène. Mais l'environnement bancaire européen étant sensiblement égal à celui de la zone UEMOA, et les risques de fraudes potentiels étant les mêmes, nous avons dans un premier temps recensé les moyens de paiement utilisés actuellement dans les pays de l'union, leur niveau de sécurité, les faiblesses et les risques de fraude dont ils font l'objet. Ensuite nous avons fait des recommandations au plan sécuritaire, basées sur l'expérience européenne concernant le fonctionnement de ces nouveaux moyens de paiement afin de les rendre plus fiables.

CESAG - BIBLIOTHEQUE

DEUXIEME PARTIE
SITUATION DES MOYENS DE PAIEMENT DANS LA ZONE EURO

CESAG BIBLIOTHEQUE

I- ANALYSE DE LA SITUATION DES MOYENS DE PAIEMENT DANS LA ZONE EURO

Encore marquée par les spécificités culturelles, l'Europe des moyens de paiement est un enjeu pour les banques européennes. C'est pourquoi elles ont créé l'European Payment Council (EPC). Il s'agit pour les Européens, d'harmoniser le cadre des différents moyens de paiement scripturaux et d'interconnecter les systèmes. En effet si les systèmes de paiement fonctionnent bien au niveau national, toutes les règles nécessaires ne sont pas encore en place, pour faire de la zone euro un nouvel espace de paiement « domestique ».

Créé en juin 2002, à l'initiative des banques européennes, l'EPC a pour objectif de définir ce que seront demain les systèmes et moyens de paiement en Europe. Pour cela, il se fonde sur les besoins des consommateurs européens et aborde l'ensemble des problématiques des moyens de paiement : virements, chèques, cartes, commerce électronique, grandes infrastructures, automatisation, sécurité, etc.

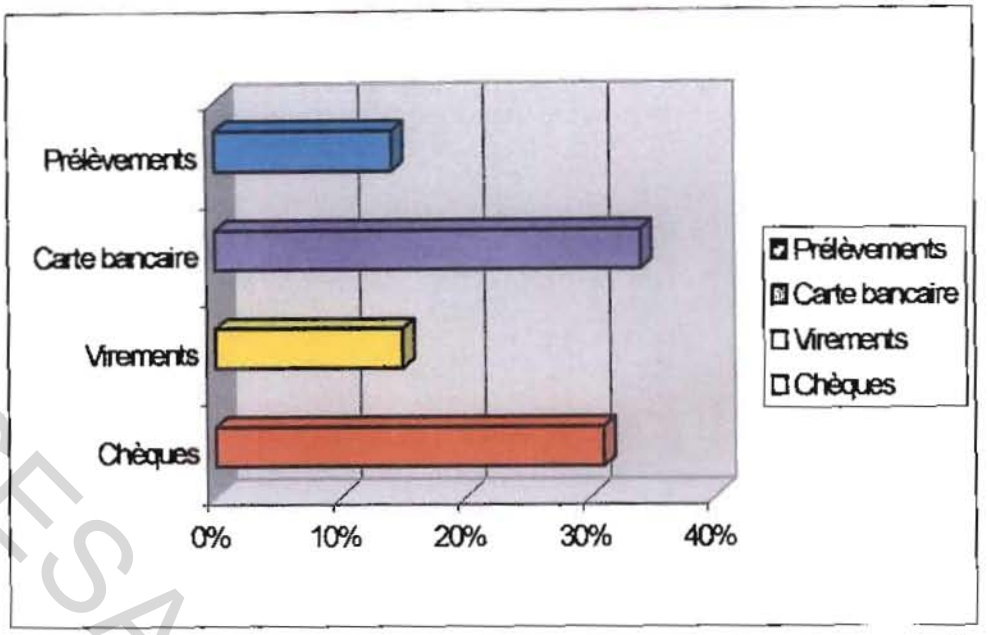
L'utilisation des moyens de paiement restera toutefois marquée encore longtemps par les habitudes culturelles. On observe qu'un Européen choisit des moyens de paiement différents selon qu'il effectue des achats dans son propre pays ou dans un autre pays de la zone euro.

Les cartes de paiements et retraits aux Distributeurs Automatiques de Billets (DAB) sont plébiscitées à plus de 83% pour les opérations transfrontalières, alors qu'elles représentent 34% des moyens utilisés pour les achats au sein d'un même pays de la zone euro. Pour les paiements domestiques, après la carte, le virement est le moyen le plus utilisé dans l'ensemble de la zone euro. En France, il progresse de 3% et constitue 15% de l'ensemble des paiements scripturaux, mais pour un montant dont la part varie peu, avec 35% du montant total des échanges. Le chèque ne vient qu'en quatrième position avec 15.5% des paiements domestiques européens. Le porte monnaie électronique et les e-paiements ont fait une apparition en 2001 avec 0.2% des paiements.

Derrière ces moyennes européennes, se cachent de fortes divergences d'utilisation selon les pays. La France a ainsi une position très particulière en Europe. C'est en effet, de loin, la plus grande consommatrice de chèques. Ils représentent environ 31% des moyens de paiement utilisés en France contre 15.5% pour la moyenne des pays de la zone euro. En 2003 elle représente 52% des chèques émis dans l'Union, contre 3.8% pour l'Allemagne. Il est donc logique que les chèques, moyens de paiement peu connus dans les pays européens, ne soient pas retenus pour les paiements transfrontaliers.

CESAG - BIBLIOTHEQUE

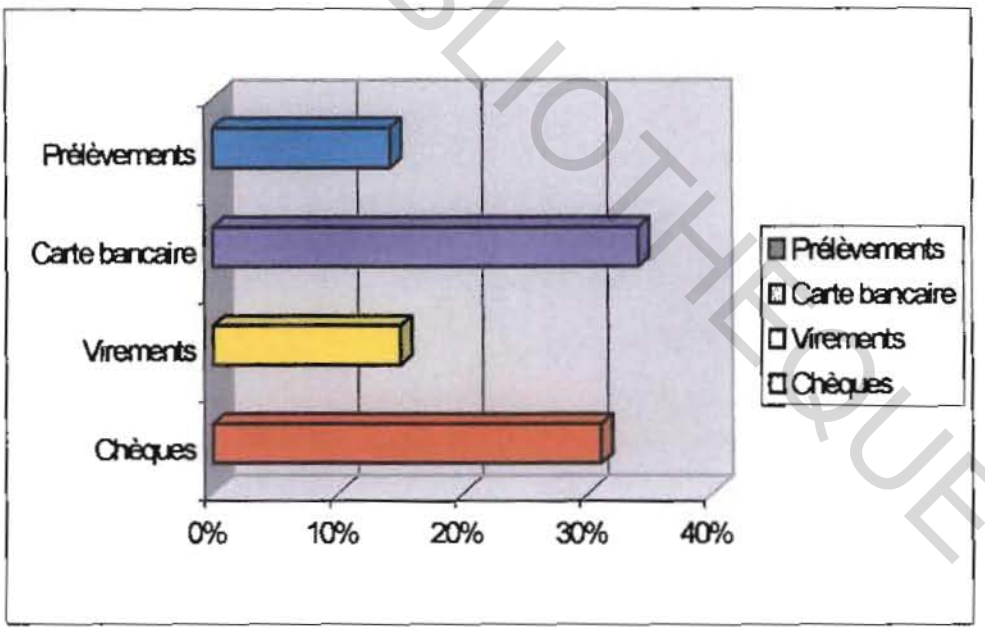
Graphique 1



FRANCE : opérations échangées dans le système bancaire en 2003[2]

CESAG - BIBLIOTHEQUE

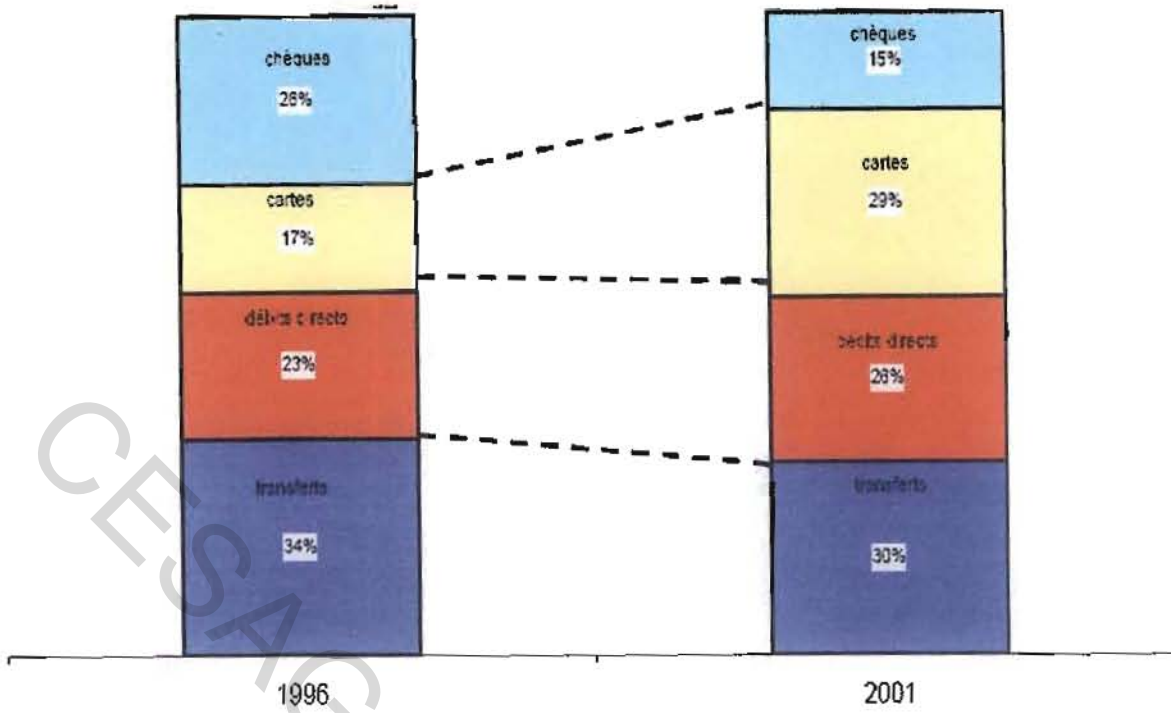
Graphique 2



Zone EURO : opérations échangées en 2003

[2] source : GSIT, EFMA, SWIFT, TARGET, ECB stat, McKinsey

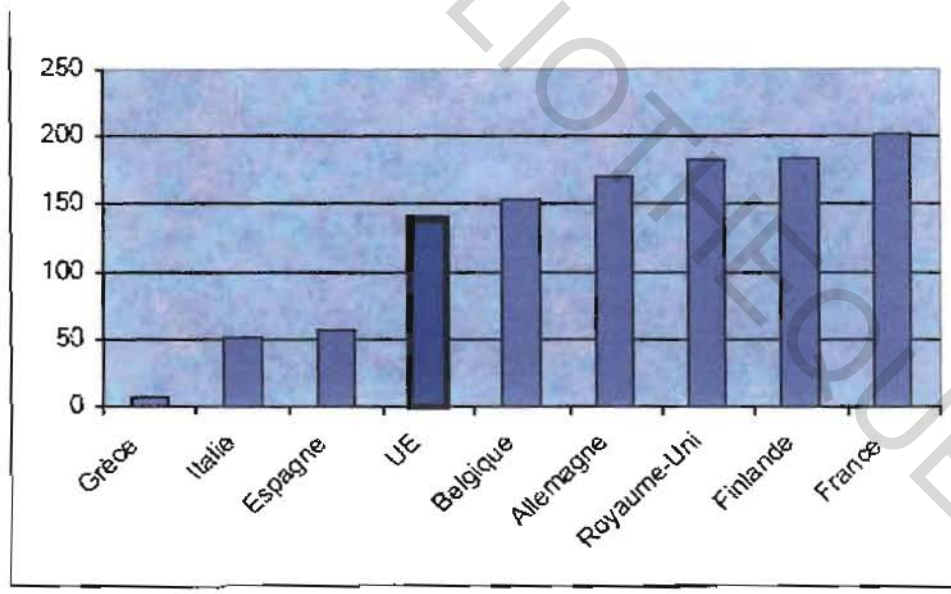
Graphique 3



Répartition des moyens de paiement scripturaux dans l'UE en % de volume

Evolution 1996 – 2001[3]

Graphique 4



Nombre annuel de transactions scripturales par habitants en 2001[4]

[3] Source : Blue Book de la BCE, addendum sur les chiffres 2001, publié en septembre 2003
[4] Source : Blue Book de la BCE, addendum sur les chiffres 2001, publié en septembre 2003

CESAG - BIBLIOTHEQUE

En 2003, 10.6 milliards d'opérations de paiement ont été échangées dans les systèmes interbancaires européens, pour un montant de 4642 milliards[5] d'euros, c'est plus de 3 fois le PIB français en 2002, l'enjeu est énorme. Pour assurer un niveau de sécurité à la hauteur de ces enjeux pour tous les moyens de paiement, les entreprises bancaires investissent dans les technologies les plus efficaces (carte à puce, cryptologie, dématérialisation des chèques et effets de commerce…), et incitent les utilisateurs à mieux se protéger eux-mêmes (terminaux d'encaissement, utilisation personnelle du code).

Ainsi, les mesures de sécurité qui ont été prises pour fiabiliser ses instruments de paiement sont les suivantes :

CESAG BIBLIOTHEQUE

I-1- Sécurité des chèques

Du fait de son support papier, et les informations non cryptées, le chèque comporte des faiblesses en terme de sécurisation. On évalue à 0.3% la part des chèques rejetés en janvier 2004 en France, dont environ 86% pour provision insuffisante, l'autre part comportant des chèques volés ou contrefaits. L'Echange Image Chèque (EIC) a été mis en place pour dématérialiser le traitement des chèques. En diminuant fortement la circulation et les manipulations des vignettes (chèques), il permet de limiter les risques de fraude. La profession s'efforce également, avec les partenaires de la filière chèques, de renforcer la sécurité des vignettes physiques.

I-2- Sécurité des virements et prélèvements

Les virements et les prélèvements échangés dans le système interbancaire totalisent 3.2 milliards d'opérations en 2003. Ces deux instruments sont dématérialisés et sont construis de telle sorte que les règles contractuelles banques/clients assurent une très forte sécurité pour le client.

Concernant le virement, les banques ont mis en place des dispositifs afin de vérifier l'identité du donneur d'ordre et son habilitation à faire un virement sur le compte destinataire. Il s'agit d'éviter toute usurpation de coordonnées bancaires en amont, lors de l'envoi d'un ordre de virement, et en aval de s'assurer qu'il n'y ait pas de détournement de fonds.

Le prélèvement est soumis en France à des règles professionnelles très strictes, qui lui assurent un taux de fraude minime. Les créanciers destinataires des prélèvements sont par exemple identifiés et enregistrés auprès de la Banque de France.

[5] Source : Actualité Bancaire, Numéro 489, 27 avril 2004

I-3- Sécurité des cartes bancaires

Ce jeune moyen de paiement, né il y a 30 ans, a bénéficié de toutes les avancées technologiques. C'est en France que l'avancée technologique est la plus notoire. Grâce à la carte à puce et aux règles contractuelles définies par le GIE Carte Bancaire, le taux de fraude sur les cartes bancaires CB est très faible au niveau national. En 2003, la fraude en France, s'est élevée à 70 milliards d'euros, soit 0.036% du montant des transactions[6]. L'enjeu consiste désormais à réduire la fraude au niveau transfrontière, où elle s'élève à plus de 1%. Les fraudes sur les paiements par carte sont principalement dues à l'utilisation des pistes magnétiques dont sont encore équipées les cartes. C'est le cas en particulier pour les opérations effectuées à l'étranger dans des pays qui n'ont pas encore adopté la technologie de la puce pour leurs cartes de paiement. Il sera mis un terme à ce type de fraude que lorsque tous les pays, notamment ceux de l'UE l'auront adopté. De ce point de vue, les normes internationales EMV[7], définies conjointement par les trois grands émetteurs de cartes Europay, MasterCard et Visa, ont été édictées pour lutter contre la fraude et promouvoir la technologie puce. En France, la migration des cartes bancaires à la norme EMV s'est accélérée au cours de l'année 2003, l'objectif étant de l'achever pour l'ensemble du parc des cartes à la fin 2006.

I-4-Sécurité des paiements en ligne

La sécurité des transactions de paiement par cartes sur l'Internet va également être améliorée avec la mise en œuvre du protocole 3D Secure. Ce protocole suppose une authentification préalable du porteur de la carte par son émetteur lors d'une transaction de paiement, selon des méthodes à la convenance de l'émetteur.

Plusieurs textes réglementaires en France et en Europe définissent le cadre juridique des transactions en ligne et les encouragent, comme la loi sur la sécurité quotidienne. Les banques participent au renforcement de la sécurité en ligne, qui repose à la fois sur des investissements technologiques et sur une clarification des responsabilités de chacun. Ainsi dans le cadre de la consultation de la Commission Européenne sur le « New Legal Framework[8] », les banques ont insisté sur la nécessaire dissociation entre la relation client/commerçant et l'exécution du paiement afin d'éviter toute confusion dans la mise en jeu de responsabilités en cas de litige commercial.

[6] Source : GIE Carte Bancaire.

[7] Nouvelles formes de sécurité, basées sur le renforcement de la sécurité de l'authentification de la transaction avec l'algorithme triple DES quatre vingt dix (90) bits. Quant à la signature RSA, elle va passer à mille vingt quatre (1024) bits.

[8] Ensemble de règles juridiques moderne et complet applicables à tous les services de paiement dans l'UE.

CESAG - BIBLIOTHEQUE

II- Cadre juridique et légal

Les différences entre les législations nationales peuvent se révéler préjudiciables au déploiement des infrastructures de dimensions européennes et à l'harmonisation des règles concernant les moyens de paiement. C'est pourquoi la Commission Européenne a lancé une réflexion sur le « Nouveau Cadre Juridique pour les paiements dans l'UE », qui a été soumis à consultation publique le 3 décembre 2003.

CESAG - BIBLIOTHEQUE

TROIXIEME PARTIE

SITUATION DES INSTRUMENTS DE PAYEMENT SCRIPTURAUX DANS L'UEMOA

CESAG - BIBLIOTHEQUE

I- ETAT DES LIEUX

Au 28 juillet 2004, le nombre de banques agréées par les autorités monétaires était de 74 contre 24 pour les établissements financiers.

Tableau1[9]

Répartition des établissements de crédit par pays

	31 décembre 2001				31 décembre 2002*			
	Banques	Ets. Fin. **	Guichets P1	Guichets P2	Banques	Ets. Fin.**	Guichets P1	Guichets P2
Bénin	6	2	33	5	7	1	32	0
Burkina	7	5	78	39	7	5	76	39
Côte d'Ivoire	16	6	162	3	16	6	159	1
Guinée-Bissau	3	0	6	0	2	0	5	0
Mali	9	4	66	1	9	4	65	1
Niger	7	1	21	0	7	1	21	0
Sénégal	11	4	98	1	11	3	106	2
Togo	7	4	100	2	7	4	99	1
UMOA	66	26	564	51	66	24	563	44

N.B. P1 = guichets permanents ; P2 = guichets périodiques.
* : sur la base des arrêtés d'agrément ou de retrait d'agrément.
** : établissements financiers.

Répartition des établissements de crédit par pays

Les moyens de paiement scripturaux les plus usités au sein de l'UEMOA sont : le chèque, le virement, les effets de commerce et la carte bancaire.

I-1- LE CHEQUE

«Principal instrument de paiement après la monnaie fiduciaire, le chèque constitue le moyen de paiement le plus usité dans les transactions économiques des pays de l'UEMOA, puisqu'il représente 85% du volume et 62% de la valeur des paiements scripturaux»[10]. Il est la façon la plus simple pour un détenteur de compte d'utiliser ses fonds, et peut être transmis à son destinataire par la Poste.

Les caractéristiques de la forme du chèque sont les suivantes[11] :

- les textes pré imprimés sur le chèque doivent être rédigés dans la langue de travail des pays de l'UEMOA.

[9] Source : site Internet BCEAO
[10] Source : présentation systèmes et moyens de paiement/Kwassi/DSP/BCEAO
[11] Source : Plénière état des lieux EIS du 12/03/2004 – BCEAO/DSP

CESAG - BIBLIOTHEQUE

- le format du chèque est de 80 mm (19 sixièmes de pouce) en hauteur et de 175 mm (69 dixième de pouce) en longueur. Ces dimensions sont tolérées dans l'instruction n° 01/CIP du 1er février 1999 de la BCEAO.

Le chèque comprend deux parties : le chèque proprement dit et la bande réservée à l'impression des caractères magnétiques, située en bas de la formule et sur toute sa longueur.

Le papier pour l'impression en caractères magnétiques doit être sans bois, dépourvu de particules magnétisables, de bonne résistance mécanique, opaque, suffisamment rigide et apte à l'impression, à l'écriture manuelle, au marquage en caractères magnétiques et au passage sur les matériels spécifiques. Le grammage de papier doit se situer entre 90 et 95 grammes par mètre carré.

Le marquage est effectué aux moyens des caractères dits CMC7 (Caractères Magnétiques Codés à 7 bâtonnets), définis par la norme internationale ISO (Organisation internationale de la normalisation). La hauteur des caractères CMC7 est de 3 mm. Les couleurs des caractères et du fond du chèque doivent permettre une lecture facile des informations.

Actuellement, dans le souci de moderniser l'environnement de son système de paiement, la Banque Centrale des Etats de l'Afrique de l'Ouest est en train de migrer petit à petit du système actuel d'échange manuel des valeurs papiers, jugé peu fiable et présentant par la même occasion beaucoup de risques de fraude, vers un système d'échanges d'images scannées de chèques, lettres de change et billet à ordre qui est plus sûr, avec un délai d'encaissement rapide.

I-2- LES VIREMENTS

Ils sont principalement utilisés dans le cadre d'opérations intra bancaires, interbancaires ou internationales. Leur part relative dans les paiements scripturaux est de 13% en terme de volume et 29% en valeur[12].

Il s'agit du moyen de paiement privilégié dans les transactions interbancaires. Il passe aussi par la chambre de compensation. Certaines entreprises préfèrent ce moyen de paiement surtout en ce qui concerne les salaires et les nivellements des comptes entre le siège et les succursales.

Cependant, le mandat postal est préféré à ce mode de paiement par les particuliers pour les transferts de fonds, même lorsque le bénéficiaire réside à l'étranger.

[12] Source : présentation systèmes et moyens de paiement/Kwassi/DSP/BCEAO

CESAG - BIBLIOTHEQUE

I-3- LES EFFETS DE COMMERCE

L'utilisation des effets de commerce[13] est très limitée dans les transactions commerciales parce que très souvent les échéances ne sont pas respectées par les tirés. Ces instruments sont le plus souvent utilisés par la clientèle commerciale des banques dans les transactions avec l'étranger.

La part relative de ces instruments dans les moyens de paiement scripturaux est estimée à près de 2% en volume et moins de 6% en valeur.

Nous avons principalement deux types d'effets de commerce : la lettre de change et le billet à ordre.

La lettre de change est un titre par lequel une personne dénommée tireur donne l'ordre à une autre personne appelée tiré de payer, à une date convenue, une somme déterminée, à un bénéficiaire qui peut être soit le tireur lui-même, soit un tiers (suite à un endos).

Conformément à l'article 149 du règlement n° 15/2002/CM/UEMOA, la lettre de change contient :

- la dénomination de la lettre de change inséré dans le texte est exprimée dans la langue employée pour la rédaction du titre ;
- le mandat pur et simple de payer une somme déterminée ;
- le nom de celui qui doit payer (tiré) ;
- l'indication de l'échéance ;
- l'indication de la date et du lieu où la lettre de change est créée ;
- la signature de celui qui émet la lettre de change (tireur). Cette signature est soit apposée à la main, soit par tout procédé manuscrit.

La lettre de change dont l'échéance n'est pas indiquée est payable à vue.

[13] Source : Plénière état des lieux EIS du 12/03/2004 – BCEAO/DSP

CESAG - BIBLIOTHEQUE

Le billet à ordre est un titre constatant l'engagement d'une personne dénommée « le souscripteur » de payer, à une date convenue, une somme déterminée, à l'ordre d'une personne dénommée «le bénéficiaire».

Conformément à l'article 228 du règlement n°15/2002/UEMOA, le billet à ordre contient :

- la promesse pure et simple de payer une somme déterminée ;
- l'indication de l'échéance ;
- l'indication du lieu ou le paiement doit s'effectuer ;
- le nom de celui auquel l'ordre doit être fait ;
- l'indication de la date et du lieu où le billet à ordre est créé ;
- la signature de celui qui émet le billet à ordre (souscripteur).

Le titre dans lequel une des mentions ci-dessus fait défaut, ne vaut pas comme billet à ordre.

I-4- LA CARTE BANCAIRE

La carte bancaire est souvent une carte de débit, car principalement utilisée par la clientèle pour les retraits d'espèces auprès des distributeurs automatiques de billets. Elle est faiblement utilisée en raison de sa méconnaissance par le public ainsi que la réticence des commerçants à l'accepter comme moyen de règlement.

Son utilisation reste encore marginale par rapport aux autres moyens de paiement scripturaux. Il est recensé en 2002, environ 160.000 cartes pour la Côte d'Ivoire, 95000 pour le Sénégal et 221360 pour l'ensemble des pays de l'UEMOA, soit à peine 1% du volume des transactions[14]. Dans certains pays comme le Niger, la carte est inexistante tant au niveau de l'émission que de l'acceptation. L'explication majeure de cette faible utilisation de la carte bancaire dans la zone UEMOA peut se justifier par :

- un sous équipement, avec un réseau de télécommunication parfois défaillant et peu développé hors zones urbaines ;

[14] Source : présentation systèmes et moyens de paiement/Kwassi/DSP/BCEAO

CESAG - BIBLIOTHEQUE

- une absence totale d'interbancarité ;
- une concentration importante de l'implantation des DAB/GAB en ville ;
- un nombre de commerçants affiliés à un réseau cartes bancaires faible ;
- un manque de communication auprès des différents intervenants (porteurs et commerçants) ;
- un manque de confiance des commerçants dans les moyens de paiement scripturaux ;
- une faible bancarisation de la population ;
- l'importance du marché informel au sein des pays de la sous région (20 à 30% en moyenne, 70% pour le Niger) ;
- un réseau d'acceptation très limité.

Nous constatons que seulement 15% des comptes ouverts par des particuliers sont associés à une carte.

Par ailleurs nous distinguons deux types de cartes bancaires utilisées dans les pays de l'union : les cartes nationales et les cartes internationales.

La quasi-totalité des cartes émises sont des cartes privatives, adossées à un compte chèque ou un compte d'épargne, utilisées principalement pour effectuer des retraits d'espèces auprès des Distributeurs Automatiques de Billets (DAB) et Guichets Automatique de Banque (GAB). Les cartes nationales sont de deux types : la carte de retrait gratuite adossée à un compte d'épargne et la carte de retrait ou de retrait paiement payante adossée à un compte chèque.

Généralement toutes les cartes sont à débit immédiat avec autorisation au premier franc, et assorti d'autorisation de découvert dont le montant varie selon le type de carte.

En règle générale, la carte bancaire est un instrument de retrait de salaire. Les cartes de retrait sont utilisées sur les DAB/GAB 2 fois par mois pour effectuer des transactions,

CESAG - BIBLIOTHEQUE

soit pour le retrait du salaire et le retrait du découvert autorisé. Néanmoins, les banques poussent les consommateurs à utiliser les cartes dans les transactions courantes aux moyens de mesures incitatives tels que : la gratuité des opérations ou le découvert autorisé. Mais malgré cela des difficultés quotidiennes sont rencontrées par les porteurs de carte, résultant de l'insuffisance du nombre d'automates mal répartis sur l'étendue du territoire, ainsi que de l'indisponibilité fréquente des machines.

Toutefois, grâce aux efforts déployés par la BCEAO dans le but de moderniser les moyens de paiement, des moyens considérables ont été mis en place pour vulgariser l'utilisation de la carte bancaire dans la sous région notamment grâce au projet de création d'un système interbancaire régional de paiement par carte. Ceci afin de réduire la circulation des espèces, de faciliter les transactions internationales par cartes, d'assurer la sécurité globale du système, de disposer d'un système bancaire moderne grâce à l'adoption d'une nouvelle génération de carte bancaire à microprocesseur respectant les normes EMV et donc plus fiable que celle à piste magnétique utilisée jusqu' à présent.

II- GESTION DES RISQUES

II-1- LA CARTE BANCAIRE

Peu de fraudes sont constatées jusque là, mais de nombreux risques subsistent. Seules les cartes privatives à usage de retrait ont fait l'objet de fraudes de faible envergure.

Par contre les fraudes sur les paiements, sont beaucoup plus importantes sur les cartes internationales, et se présentent essentiellement sous forme de contrefaçon. Notons que si jusqu'ici les pays de l'UEMOA ont été épargnés par des fraudes à grande échelle, ils doivent néanmoins anticiper et se préparer contre les différents types de fraudes qui sévissent ailleurs dans le monde dont voici quelques exemples :

Une première technique de fraude consiste à dupliquer les cartes bancaires à piste magnétique. Il suffit d'utiliser un lecteur encodeur, en vente libre dans le commerce. On passe la carte dans l'appareil, puis une deuxième carte pour dupliquer la bande magnétique; la copie se fait en quelques instants. Le lecteur encodeur ressemble à n'importe quel terminal. On peut obtenir, par ce biais, une carte "blanche", morceau de plastique rectangulaire sans décoration, qui ne porte que la piste magnétique. Si en plus, on a réussi à relever le code secret à 4 chiffres, la carte peut alors être utilisée dans certains distributeurs automatiques d'essence, automates de distribution de cassettes vidéo. La quasi totalité des distributeurs n'utilisent que la piste magnétique, on peut alors opérer des retraits, moins facilement faire des achats, à moins que le commerçant ne soit lui-même complice. Il est également possible de créer facilement

CESAG - BIBLIOTHEQUE

une carte à piste magnétique si on est en possession du numéro à seize chiffres et du code à quatre chiffres.
Une autre technique de fraude qui fut retentissante, est celle dite méthode Humpich[15] avec la Yescard (Simulacre de carte à puce avec numéro de porteur inexistant).

Humpich est un ingénieur électronicien, qui dénonça publiquement les faiblesses de la carte à puce en réalisant de fausses cartes. Il lui a suffit d'explorer la bande magnétique et la puce de ses cartes de crédit, et de reconstituer le mécanisme de cryptage utilisé par les banques.

Dans un premier temps, il a généré aléatoirement un numéro de carte à 16 chiffres correspondant à une banque française, et a choisi au hasard un nom de porteur ainsi qu'une date d'expiration de la carte dans le futur. Puis il a encodé toutes ces informations au format hexadécimal, ce qui lui aurait permis d'obtenir un numéro de quarante huit chiffres décimaux appelé identifiant. Une valeur d'authentification de quatre vingt seize chiffres décimaux de 320 bits a été obtenue par suite d'une multiplication de l'identifiant par un nombre. Puis les deux numéros de quarante huit chiffres et de quatre vingt seize chiffres sont alors stockés sur cette carte à puce blanche programmable. Programmer une carte à puce blanche ne pose pas vraiment de difficultés, on peut facilement trouver le matériel nécessaire, et en plus, le système est le même que pour les décodeurs satellites pirates.

Mais quelles étaient donc les principales failles du système[16] ?

Le code secret à quatre chiffres ne sert pas pour l'authentification, il ne sert que pour insérer une transaction dans l'historique des transactions (ce qui est quasiment inutile). Les cartes émises depuis novembre 1999 comportent deux valeurs d'authentification : l'une de 320 bits créée à l'aide de la clé cassée révélée sur Internet le 04 mars 2000, l'autre de 768 bits. Comme toutes les données servant à l'authentification sont situées dans des zones publiques accessibles sans le code, toutes les cartes bancaires à puce peuvent être recopiées à l'insu du porteur et retranscrites sur un émulateur dit « Yescard ».

La Yescard permet d'effectuer des transactions sur tous les automates ne faisant que lire l'identifiant et la valeur d'authentification sur la puce (automates des pompes à

[15] Serge Humpich : Informaticien électronicien et né en 1963, en Alsace, Serge Humpich est diplômé de l'Institut National des Sciences Appliquées, et a travaillé comme ingénieur chez MCDonnell Douglas, puis pour le groupe GFI. Surnommé le « pirate bleu » suite à la fabrication de fausses cartes bancaires, il a été licencié pour faute grave.

[16] Source : www.parodie.com/humpich/

CESAG - BIBLIOTHEQUE

essence, voire terminaux chez les commerçants) et pour des valeurs inférieures au seuil de vérification. Tout code tapé est considéré comme bon, à partir du moment où la banque n'est pas appelée par le terminal pour vérification. Le code ne sert en fait qu'à parvenir au journal des opérations stockées sur la carte. La fraude ne sera signalée que lorsque le commerçant enverra le compte rendu des transactions à la banque.

Les banques n'ont exploité aucune des sécurités de la puce. Le code aurait dû servir à restreindre l'accès des secrets (la valeur d'authentification et l'identifiant composé du numéro de carte bancaire) aux seuls titulaires du code secret, mais ces secrets sont accessibles sans le code. La puce peut faire des calculs cryptographiques complexes permettant de prouver qu'elle détient un secret sans le révéler, ce qui permet d'éviter les attaques par clonage de carte. Cette possibilité de la puce n'a pas non plus été utilisée dans les cartes bancaires.

Dans une perspective de déploiement en masse de l'instrument carte au niveau sous régional, cela favoriserait une plus grande recrudescence de la fraude sur les cartes bancaires au sein de l'UEMOA, puisque le risque pour le fraudeur de se faire prendre sera moins important et les potentialités de gains accrues.

Mais peut être aussi que l'interbancarité pourrait constituer une parade contre la fraude, si tous les pays de l'union mettent en place une politique sécuritaire commune pour lutter contre ce fléau. Par ailleurs le passage aux normes internationales Europay MasterCard Visa (EMV), ainsi que l'adoption immédiate de carte à microprocesseur qui s'appuie sur des standards internationaux, sont autant de moyens pour lutter contre la contrefaçon et la fraude au sein des pays de l'UEMOA.

II-2- LE CHEQUE

Pour des mesures de sécurité, les établissements de crédit assujettis, intègrent lors de l'impression de leurs formules, des éléments de contrôle dans les caractéristiques du papier, de l'encre et des caractères de personnalisation. En plus de la norme sur la forme et les mentions obligatoires, le chèque se caractérise par son graphisme, les encres utilisées (leur couleur, leur intensité et leur sensibilité éventuelle) ainsi que le papier utilisé et sa sensibilité éventuelle. Il en est de même pour le choix du graphisme, du procédé d'impression, sans oublier les techniques et précautions qui pourront dissuader les fraudeurs.

A toutes ces mesures de sécurité pour minimiser le risque, s'ajoute la migration du traitement chèque papier, vers le traitement du chèque scanné qui permet d'échanger les chèques images sous forme de fichier informatique entre établissements de crédits, garantissant ainsi une plus grande sécurité, une plus grande fiabilité et surtout une

CESAG - BIBLIOTHEQUE

rapidité exceptionnelle dans les échanges de valeurs. Du fait de son support papier, et les informations non cryptées, le chèque comporte des faiblesses en terme de sécurisation. L'Echange Image Scannée (EIS) a été mis en place pour dématérialiser le traitement des chèques. En diminuant fortement la circulation et les manipulations des vignettes (chèques), il permet de limiter les risques de fraude.

III- SECURISATION DES MOYENS DE PAIEMENT SCRIPTURAUX

III-1- SECURISATION TECHNIQUE

III-1-1- LA CARTE BANCAIRE

Il existe deux types de cartes :

- La carte à piste magnétique ;
- La carte à microprocesseur, communément appelée carte à puce.

Quelque soit le type de carte, la sécurité est très importante, dès lors qu'il s'agit de paiement électronique. Ainsi, on parle de transaction sécurisée, lorsque deux conditions sont réunies :

- L'établissement bancaire doit connaître de manière certaine l'émetteur du paiement.
- La transaction ne peut être modifiée, entre l'instant où elle a été émise et l'instant où elle sera traitée par la banque.

La transaction par carte est sécurisée par le principe de la signature cryptographique qui permet à la fois l'authentification de l'instrument de paiement, ainsi que l'intégrité de la transaction.

Néanmoins, il existe au sein de l'UEMOA des failles qui occasionnent le piratage des cartes à piste magnétique. Ainsi, Il est très aisé de falsifier ce type de carte, pour peu qu'on possède le matériel et la technologie adéquate. Ce qui n'est pas le cas de la carte à microprocesseur, qui nécessite un équipement «hardware» très sophistiqué, sans compter le coût qu'une telle opération pourrait engendrer. A cela il faudra ajouter la vigilance des banques, qui vérifient en permanence la logique des transactions.

Comment est sécurisée une carte à puce ?

CESAG - BIBLIOTHEQUE

- Le premier élément de sécurité d'une carte est le code confidentiel. Sa vérification se fait de la manière suivante : le terminal de paiement envoie une requête à la carte pour demander si le code entré par l'utilisateur est correcte, après un calcul, la carte répond par oui ou par non.

- La deuxième étape concerne l'authentification de la carte. Une fois introduite dans le terminal de paiement, la carte doit s'authentifier par une signature RSA (du nom des trois chercheurs qui sont à l'origine de la création de cette clé en 1977 : Rivest, Shamir et Adleman), inscrite sur la puce. Cette signature comporte quatre vingt seize (96) chiffres, et de ce fait identifie de façon unique la carte. Sa reproduction est quasiment impossible.
  Mais un problème subsiste : la faiblesse de cette clé. Elle fait seulement 320 bits, or une clé de 512 bits a été déjà cassée en 1999.

- Enfin, vient l'authentification de la transaction.
  Lors d'une transaction avec une carte à puce, la procédure est authentifiée par un numéro de seize (16) chiffres, le même qui apparaît sur les tickets. Ce numéro a pour rôle principal de brouiller toutes les informations relatives à la transaction, en appliquant un cryptage DES cinquante six (56) bits, ce qui assure l'intégrité de la transaction.

Face à toutes ces insuffisances sécuritaires de cette ampleur, il est impératif pour le système bancaire de l'UEMOA de renforcer la sécurité de ses cartes bancaires, en adoptant :

- les nouvelles générations de cartes à puce respectant la norme EMV en remplacement des cartes à piste magnétique actuellement usitées dans les pays l'Union. C'est un standard qui propose plusieurs types de protocoles en matière de sécurité. En effet EMV propose de nouvelles formes de sécurité, basées sur le renforcement de la sécurité de l'authentification de la transaction avec l'algorithme triple DES quatre vingt dix (90) bits. Quant à la signature RSA, elle va passer à mille vingt quatre (1024) bits.
  La technologie à puce offre plus de potentialités par rapport à la technologie à piste magnétique dans le domaine sécuritaire

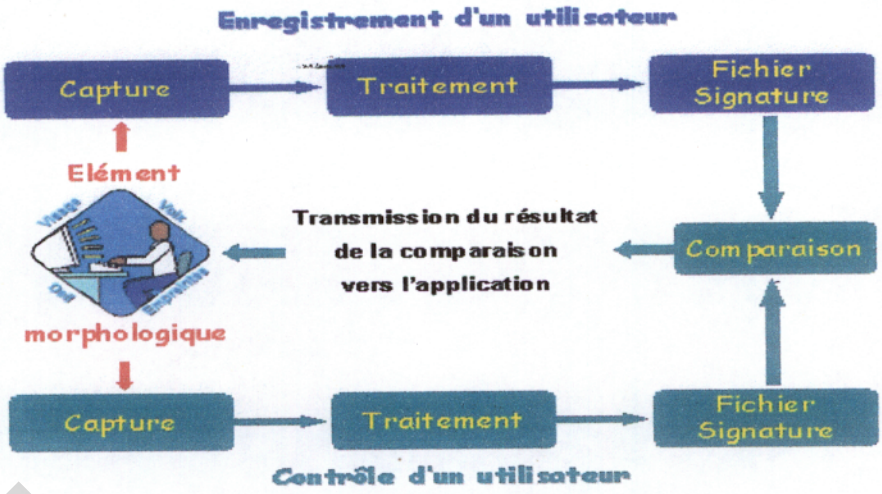
CESAG - BIBLIOTHEQUE

d'authentification de la banque, du support et du porteur (lutte contre la fraude et la contrefaçon «abusive»).

- Une autre solution pour la sécurisation des cartes bancaires et non des moindres, est la biométrie associée au système interbancaire de paiement par cartes. La biométrie est la science qui permet d'identifier automatiquement un individu en se basant sur ses caractéristiques physiologiques ou comportementales. Généralement, on distingue deux catégories de méthodes d'authentification biométrique : les méthodes basées sur les caractéristiques physiques telles que visage, voix, iris, rétine, pouce, forme de la main et de l'oreille, ADN, système veineux et celles basées sur les caractéristiques comportementales comme la signature, la manière de marcher ou de taper sur un clavier *(keystroke dynamics)*.
  Quasiment tout, dans l'anatomie ou le comportement d'un individu, peut être transformé en un code informatique permettant de l'identifier.

  Un système d'acquisition équipé d'un capteur est utilisé pour acquérir une caractéristique spécifique de l'utilisateur, par exemple : un lecteur d'empreintes digitales pour les empreintes. A partir d'un élément biométrique propre à un individu on détermine un gabarit, c'est-à-dire une suite numérique qui caractérise l'élément biométrique et c'est le gabarit qui est conservé et non l'image de l'élément biométrique à proprement parler. La technique d'élaboration du gabarit est propre à chaque éditeur de logiciel biométrique. Pour reconnaître un individu, on extrait des paramètres de l'image photographiée (empreinte, face, iris...) puis on compare le gabarit obtenu avec tous les paramètres précédemment extraits et sauvegardés. Les différentes étapes du processus d'identification d'un individu sont présentées à travers ce schéma :

CESAG - BIBLIOTHEQUE



Source : www.biometrie.online.fr

La réalisation d'un tel système parait futuriste, mais pourrait constituer un moyen de lutte efficace contre les vols de cartes et les fraudes. Toutefois les recherches effectuées n'ont pas permis d'avoir des informations précises sur ce système. Cependant, même s'il a le désavantage d'utiliser une technologie trop sophistiquée et donc très coûteuse pour les pays de la zone UEMOA, il n'en demeure pas moins qu'une attention toute particulière lui soit portée, dans une perspective d'optimiser la fiabilité et la sécurité du système de paiement par cartes bancaires.

Ainsi, à partir du processus d'identification schématisé ci dessus et traditionnellement utilisé par les forces de police ainsi que les services d'immigration, nous proposons la procédure suivante pour les transactions par cartes bancaires:

- lors de la personnalisation de la carte bancaire par le concepteur, des caractéristiques physiques uniques de l'individu (visage, voix, iris, rétine, pouce, forme de la main), doivent être intégrées sur la puce de la carte ;

- Les terminaux de paiement sont équipés de capteurs utilisés pour acquérir une caractéristique spécifique de l'utilisateur et capables d'identifier l'émetteur de la transaction, en confrontant les caractéristiques physiques scannées de la personne, à celles déjà stockées sur la puce électronique ;

S'il y a compatibilité, le terminal continue les autres procédures de vérification :

- L'identification du code de la carte ;

CESAG - BIBLIOTHEQUE

- L'authentification de la carte ;

- L'authentification de l'intégrité de la transaction.

Cela va permettre de réduire considérablement les fraudes abusives relatives aux retraits et paiements par cartes volées ou dupliquées. Cependant, la seule contrainte à ce moyen de sécurisation est le coût afférant à l'installation d'un tel système et à son entretien. Un coût supplémentaire qui risquerait de se répercuter sur les services offerts par les établissements bancaires à la clientèle. Toutefois ces mesures sont prises dans l'optique de renforcer l'authentification de l'émetteur du paiement, de la carte ainsi que l'intégrité de la transaction.

III-1-2- LE CHEQUE

Pour optimiser la sécurisation d'un chèque, plusieurs éléments sont à prendre en compte lors de l'impression d'un chèque :

- L'utilisation du papier sensible améliore la sécurité du chèque. Il est protégé selon différents procédés techniques à savoir :

  - l'incorporation de réactifs sensibles aux solvants organiques et aux produits chimiques ;

  - l'addition de fibres fluorescentes ;

  - l'utilisation d'un papier sans azurant optique ;

Cependant l'impression à encre grasse peut provoquer des réactions. Le contraste entre la couleur de l'encre et celle du papier est déterminant sur la teinte des chèques.

- L'utilisation d'encres sensibles, vise à protéger le chèque contre la falsification, c'est à dire contre les tentatives de modifications frauduleuses pratiquées sur les écritures. L'impression peut être protégée grâce aux types d'encres utilisées :

CESAG - BIBLIOTHEQUE

- encres sensibles aux solvants organiques et aux produits chimiques ;

- encres visibles ou invisibles, fluorescents sous ultra violet.

Une encre trop pâle ne permet pas de percevoir les défauts produits par les falsifications. En revanche, les mentions portées sur teinte foncée, peuvent être difficilement lisibles.

- L'imprimeur doit veiller au contrôle des opérations exécutées dans ses locaux et plus particulièrement :

  - la gestion et le suivi rigoureux des stocks de papiers spéciaux ainsi que des encres spéciales.

  - le contrôle de la quantité des formules effectivement imprimées, du nombre de formules livrées et de la continuité de la numérotation des formules et des séries.

  - La vérification de la qualité de l'impression, en vue d'éliminer les chèques dont le graphisme ou la teinte n'est pas conforme.

Quand à la télécompensation comme moyen de paiement électronique interbancaire, technique qui repose sur le non échange physique des valeurs compensables (chèques et effets de commerce), aussi bien le banquier présentateur que le banquier tiré sont tenus de procéder préalablement au paiement, à la vérification de certaines mentions du chèque, dont notamment la conformité de la signature du tireur au spécimen de sa signature déposée auprès de la banque tirée. Or, avec l'adoption du principe du non échange physique du chèque qui suppose la suppression de la communication de tout support physique entre les banquiers compensateurs, le banquier tiré se trouve dans l'impossibilité de contrôler la régularité du chèque, puisque seul l'enregistrement électronique lui est transmis. Ainsi, l'absence de vérification, notamment de la signature par la banque tirée, risque d'engager la responsabilité de celle-ci vis-à-vis du tireur en sa qualité de mandataire chargé du paiement et ce, dans l'hypothèse où elle règle le chèque à une autre personne que le porteur légitime (chèque volé ou falsifié). En effet, le projet de

CESAG BIBLIOTHEQUE

télécompensation a prévu de faire accompagner l'enregistrement électronique adressé à la banque tirée par une image scannée et sécurisée du chèque recto verso qui permet à cette dernière d'observer les obligations légales d'usage en la matière. La même technique de scannérisation a été également prévue pour le règlement de la lettre de change afin de permettre à la banque domiciliataire de s'assurer de l'existence de l'ordre de paiement de son client tiré.

La sécurisation des échanges interbancaires de fichiers informatiques repose sur quatre principes :

- l'authentification réciproque qui permet de vérifier l'identité des partenaires mis en relation lors de la télétransmission ;
- l'intégrité qui garantit la non altération des données lors du transport du fichier ;
- la non répudiation qui permet aux deux parties de prouver l'envoi et la réception d'une télétransmission ;
- la confidentialité qui rend impossible la lecture ou l'interprétation des données par un tiers non habileté.

La télécompensation a recours à la technique du cryptage qui permet l'échange de messages entre les opérateurs avec des codes et des clés et d'éviter ainsi la transmission de ces messages "en clair". L'utilisation de cette technique permet ainsi de satisfaire au besoin de sécurisation et de confidentialité des échanges électroniques.

III-2-SECURISATION JURIDIQUE[17]

La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a initié un important projet de modernisation des systèmes de paiement des Etats membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA). La mise en œuvre de ce projet requiert la mise en place d'une nouvelle infrastructure dont la sécurité technique doit aller de pair avec sa sécurité juridique aux plans légal, réglementaire et conventionnel. La réponse aux multiples exigences de sécurité nécessite la modernisation du cadre

[17] Source : Règlement N° 15/2002/CM/UEMOA Relatif aux systèmes de paiement dans les Etats Membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA)

CESAG - BIBLIOTHEQUE

juridique actuel par l'adoption de nouveaux textes plus appropriés, l'abrogation des textes inadéquats ou l'amélioration des textes insuffisants. La Loi Uniforme sur les Instruments de Paiement qui constitue la source principale de la réglementation des instruments de paiement dans l'espace UEMOA n'avait pas suffisamment pris en compte les progrès technologiques qui ont affecté les systèmes de paiement. De sorte qu'aujourd'hui, mis à part la carte bancaire, elle ne prend pas en charge les nouveaux instruments et procédés de paiement nés de l'évolution technologique.

En effet, cette Loi Uniforme avait été adoptée dans un contexte de méfiance généralisée à l'égard des moyens scripturaux de paiement, à savoir : le chèque, la carte bancaire, la lettre de change et le billet à ordre. Les grandes orientations de cette Loi Uniforme étaient donc axées sur la restauration de la confiance du public à l'endroit de ces moyens. C'est à ce titre qu'elle avait prévu un important dispositif visant la sécurité et la fiabilité de ces moyens de paiement. Cet objectif a justifié la mise en place d'une Centrale des Incidents de Paiement et l'introduction de certaines innovations telles que :

- le pouvoir conféré aux banques de faire leur propre police en matière de chèque sans provision ;

- l'instauration d'un système d'interbancarité à travers la promotion de la carte bancaire ;

- l'institution d'un mécanisme de Centralisation informative des Incidents de Paiement relevés sur les lettres de change et billets à ordre domiciliés en banque.

Toutefois, le développement fulgurant, dans le monde des affaires, des nouveaux modes de transfert électronique de fonds, impose une réforme qui suscite des enjeux à la mesure de l'importance des changements qui vont s'opérer dans les systèmes de paiement. Aussi, est-il nécessaire de tenir compte des problèmes nouveaux liés à l'utilisation des instruments et procédés électroniques de transfert de fonds. Ces problèmes concernent :

- l'identification et l'authentification de l'expéditeur ainsi que du destinataire des messages de données ;

CESAG - BIBLIOTHEQUE

- la confidentialité des données transmises par des supports électroniques et, par conséquent, la sécurité des échanges dématérialisés ;

- l'absence de législation appropriée sur les infractions liées aux cartes bancaires et autres instruments et procédés de paiement électronique qui peut favoriser l'utilisation de ce système moderne de paiement aux fins de fraude, d'abus et de contrefaçon ;

- l'insécurité juridique liée à la méconnaissance de la preuve électronique par le droit positif dans les Etats membres de l'UEMOA.

Le nouveau dispositif vise donc à garantir la sécurité des messages qui seront transmis. Il permet, d'une part, de prendre en considération les nouveaux instruments électroniques de paiement et d'autre part, de tirer les conséquences, au plan de la politique criminelle, de cette nouveauté, en prévoyant un traitement approprié des infractions pouvant naître de l'utilisation des nouveaux instruments de transfert électronique de fonds.

Ainsi, en ce qui concerne le chèque, la principale innovation consiste dans la mise en place d'un fichier central des incidents de paiement, au niveau de l'UEMOA, dont la gestion est confiée à la BCEAO. Les informations étant fournies par chaque banque ou établissement financier dans le but de centraliser tous les incidents de paiement, de responsabiliser et sensibiliser les établissements de crédit sur les risques potentiels dont elles peuvent être victimes, d'accélérer les échanges d'information entre les établissements de crédit et la BCEAO.

Chaque banque a la possibilité de prendre, à l'égard des chèques sans provision, des mesures d'interdiction bancaire pour une durée de cinq ans assorties d'injonction de restitution de chéquiers. Cependant, la loi permet à l'auteur de l'incident de régulariser l'opération sous réserve de paiement du montant du chèque et d'une pénalité libératoire, sans préjudice de sanctions pénales. La protection du bénéficiaire est assurée en amont, par la possibilité d'interroger directement la centrale des incidents de paiements de la BCEAO, et en aval par l'obligation du banquier de l'émetteur de délivrer au bénéficiaire un certificat de non paiement qui, signifié au tireur, vaut commandement de payer.

Les incidents de paiement relatifs à la lettre de change et au billet à ordre obéissent aux mêmes règles.

CESAG - BIBLIOTHEQUE

En ce qui concerne les cartes, pour réglementer la monétique interbancaire de l'UEMOA, la communauté bancaire et financière avec l'appui de la BCEAO, a procédé à la création d'une structure sous forme de GIE, dénommée Groupement Interbancaire Monétique, chargée d'instituer et de gérer des cartes transnationales. Le GIM-UEMOA assure les fonctions dites de gouvernance :

- Organisation de l'interbancarité;
- Elaboration des règles et procédures interbancaires;
- Pilotage du système monétique interbancaire et de son interopérabilité, aux plans administratif, et réglementaire;
- Elaboration de la politique sécuritaire du système et suivi de son application;
- Gestion de la fraude.

Quant au pilotage technique et opérationnel du système, il est assuré par le Centre de Traitement Monétique (CTM), érigé sous forme de Société Anonyme.
Les décisions de retrait de cartes pour utilisations abusives sont prises par la banque et notifiées à la BCEAO.

S'agissant du règlement des paiements électroniques, Le problème essentiel en matière de paiements électroniques est double : quand est ce qu'un paiement peut-il être considéré comme irrévocable ? Et comment prouver de manière estimée irréfutable par la loi que l'ordre de paiement a bien été effectué et émanait bien de celui qui prétend l'avoir effectué ?
L'irrévocabilité d'un ordre de paiement électronique doit être de principe dès lors que l'émetteur a été authentifié selon une procédure déterminée et sauf si l'ordre lui-même contenait de manière non équivoque un délai de révocation. Dans ce cas, ce n'est qu'après expiration de ce délai de révocation que le paiement est irrévocable, étant entendu que l'ordre de révocation doit lui-même être authentifié.
Un tel système demande que soient précisées la ou les procédures d'authentification que les parties doivent utiliser et dont le non-respect pourra autoriser un refus ou une contre passation d'opération. Cette authentification repose essentiellement sur ce qu'il est convenu d'appeler «une signature électronique» du donneur d'ordre. Cette signature est attribuée par un « organe certificateur », prestataire de service accepté par

CESAG - BIBLIOTHEQUE

les parties, sous forme cryptée, c'est-à-dire qu'elle constitue une suite numérique constituée selon des règles convenues.

Le Règlement N° 15/2002/CM/UEMOA contient la détermination du cadre général de l'utilisation de la preuve électronique dans les transactions bancaires et financières, et le renvoi à une instruction du Gouverneur de la BCEAO pour définir les règles et modalités de la certification des signatures électroniques dans la perspective du renforcement de la confiance du public en elle.

IV- QUEL CADRE REGLEMENTAIRE POUR L'EMISSION DE LA MONNAIE ELECTRONIQUE ?

Les technologies de l'information et de la communication sont de plus en plus présentes dans la société africaine. Elles s'immiscent incontestablement dans tous les domaines touchant au traitement de l'information. Il existe cependant un domaine où ce phénomène commence à peine : il s'agit de la monnaie.

La digitalisation de la monnaie, c'est à dire le procédé qui consiste à stocker des signes monétaires sur un support électronique, tend à devenir une réalité au sein des paysages financiers des pays de l'UEMOA.

La réglementation peut parfois se substituer aux forces du marché lorsqu'il y a non conformité aux lois, règles, ou le simple fait que les droits et obligations des parties engagées dans une transaction ne soient pas clairement établis . Cette substitution est-elle requise dans le cas des systèmes de monnaie électronique ?

Qu'arriverait-il si un système financier restreint de monnaie électronique s'effondrait ? Les détenteurs de monnaie électronique seraient évidemment touchés, s'ils n'arrivaient plus à utiliser la valeur mise en mémoire sur la carte pour effectuer des achats.

L'effondrement d'un vaste système polyvalent de cartes à valeur mémorisée pourrait avoir un effet «dominos» sur les détaillants et les fournisseurs et se répercuter de façon sensible sur l'économie. Un nombre substantiel de marchands et d'autres fournisseurs pourraient perdre des ventes et avoir des difficultés à payer leurs créanciers.

A la limite, la faillite d'un important système polyvalent de monnaie électronique regroupant de nombreux émetteurs et comportant des garanties réciproques pourrait engendrer des problèmes plus graves pour le système financier et de façon plus générale, pour l'économie.

Mais vu que les soldes individuels touchés sont limités, il n y a sans doute pas de risque qu'une personne perde ses économies de toute une vie ou qu'un important système de paiement s'effondre.

CESAG - BIBLIOTHEQUE

Mais on pourrait constater une perte de confiance dans l'ensemble du système financier et des répercutions négatives pour tous les systèmes de monnaie électronique, et cela est un cas préoccupant.

IV-1- RISQUES LIES A L'EMISSION DE LA MONNAIE ELECTRONIQUE

IV-1-1- RISQUE OPERATIONEL

Le risque que le système ne fonctionne pas comme prévu pour des raisons opérationnelles ou techniques. Ces risques sont les plus dévastateurs. Les risques opérationnels désignent le potentiel de pertes lié aux déficiences significatives de la fiabilité et de l'intégrité du système.

IV-1-2- RISQUE JURIDIQUE

Le risque juridique inhérent à une définition floue des droits et obligations en vertu de la loi. Il concerne surtout les violations ou la non conformité aux lois, règles ou réglementations, ou le simple fait que les droits et obligations des parties engagées dans une transaction ne soient pas clairement établis.

IV-1-3- RISQUE D'UTILISATION CRIMIELLE

Le risque d'utilisation du système à des fins criminelles, y compris la fraude, entraînant des pertes de taille pour les promoteurs du système. De puissants groupes organisés peuvent investir les ressources nécessaires pour pénétrer des réseaux monétaires parce que les gains potentiels sont énormes. En inoculant un virus, il est possible de submerger un réseau de paiement et de transférer des montants illimités de fonds à des destinations inconnues.

En plus des attaques externes, les systèmes de monnaie électronique sont exposés au risque de fraude émanant de leurs propres employés qui peuvent de manière frauduleuse acquérir des données d'authentification pour accéder aux comptes clients ou voler des cartes de stockage de valeurs électroniques.

IV-1-4- RISQUE DE REPUTATION ET DE CONFIANCE

Le risque de réputation et de confiance est essentiel à l'activité bancaire. Or, la vulnérabilité accrue des banques au risque opérationnel signifie également un accroissement du risque de réputation.

La réputation d'une banque peut être mise à mal, si des problèmes dans ses réseaux de communication, réduisent l'accès à l'information. Le risque de réputation peut affecter une seule banque ou affecter l'ensemble du système bancaire. En effet si une grande

CESAG BIBLIOTHEQUE

banque réputée et ayant fortement développé ses activités d'émission de monnaie électronique subit une forte atteinte à sa réputation suite à une défaillance de son système de monnaie électronique, la méfiance des clients à l'égard des autres banques exerçant dans le même domaine d'activité, peut se généraliser.

IV-1-5- RISQUE DE DEFAILLANCE

Les risques de défaillance d'un émetteur. La défaillance d'un émetteur de monnaie électronique peut prendre deux formes :

Tout d'abord, la défaillance peut être financière. Cette situation se produit lorsque l'émetteur est incapable de faire face à ses obligations pour des motifs de liquidité ou pour des raisons de solvabilité.

Les crises de liquidités apparaissent lorsque l'actif du bilan de l'émetteur est insuffisamment liquide pour satisfaire dans les délais prévus les demandes des commerçants voulant échanger la monnaie électronique qui leur a été remise lors de transaction en une autre forme de monnaie.

Le risque d'insolvabilité provient quant à lui du fait que l'actif est insuffisant pour couvrir la valeur de la monnaie émise.

La défaillance d'un émetteur de monnaie électronique peut aussi être d'ordre technique. L'émetteur n'a pas introduit une sécurité technique suffisante dans le processus d'émission puis de circulation de la monnaie. Ceci peut alors se traduire par la destruction accidentelle des signes de monnaie électronique ou par un fort taux de piratage et de falsification qui peuvent remettre en cause l'intégrité financière de l'émetteur.

Dans ces deux cas la défaillance peut avoir des conséquences dommageables, pour les détenteurs de monnaie électronique, mais surtout, elle peut entraîner des risques systémiques dus à la perte de confiance dans la monnaie électronique, voire dans le système bancaire et financier dans son ensemble.

Face à de tels risques de grande envergure, quel type de comportement adopter ?

L'approche du «laissez faire», qui favorise l'innovation à court terme, alors que les technologies et les marchés sont en plein développement. Le marché choisit les systèmes qui seront implantés avec succès, sans être influencé par la réglementation. La prestation de service de monnaie électronique ne serait pas monopolisée par des institutions financières réglementées, ce qui favoriserait la concurrence, la diversification des services ainsi que la prestation des meilleurs services aux consommateurs.

Le risque associé à un telle pratique est que la faillite d'émetteurs dont le fonctionnement du système est déficient pourrait porter atteinte à la confiance des consommateurs dans le

CESAG BIBLIOTHEQUE

système de monnaie électronique. La législation pourrait réagir de façon démesurée aux faillites et aux pertes en cascade subies par les clients en adoptant une loi sévère.

L'autre approche est celle «prudente». Pour cette approche, seules les institutions de dépôt réglementées pourraient émettre de la monnaie électronique. En adoptant la prudence, elle garantit la surveillance des engagements, réduit les risques de faillite de l'émetteur de monnaie électronique et par conséquent les risques systémiques éventuels.
L'inconvénient de cette approche est qu'elle pourrait freiner l'innovation et le développement de nouveaux produits, limiter la concurrence et la gamme de choix offerts aux consommateurs, éliminer la possibilité d'un régime efficace d'autorégulation.

Ces deux approches étant situées aux antipodes, le législateur doit assujettir l'activité d'émission de monnaie électronique à une réglementation prudentielle ni trop rigide, ni trop laxiste, afin de s'assurer du respect de la sécurité des paiements, et d'éviter éventuellement les effets graves de distorsions de concurrence.

IV-2- PROPOSITION DE DIPOSITIF REGLEMENTAIRE ET PRUDENTIEL [18]

1- Par monnaie électronique, il convient d'entendre une valeur monétaire représentant une créance sur l'émetteur qui est stockée sur un support électronique et émise contre la remise de fonds et est acceptée comme instrument de paiement par les personnes, autres que l'émetteur ;

2- Afin de ne pas entraîner un affaiblissement des normes prudentielles, la Commission bancaire doit limiter l'accès aux activités d'émission de monnaie électronique à l'EVUMOA (Institut d'émission de valeur électronique de l'UEMOA) ;

3- Sont autorisées à émettre des portes monnaie électroniques (PME) au sein de l'UEMOA, les Banques telles que définies par la loi bancaire, les Etablissements financiers et les Systèmes financiers décentralisés.
Les sociétés non financières telles que les compagnies de téléphones, désirant émettre et commercialiser des cartes prépayées permettant d'effectuer des paiements électroniques, doivent obligatoirement sous traiter avec les

[18] Sources : - loi du 25 février 2003, relative au statut et au contrôle des établissements de monnaie électronique/Moniteur Belge 07.03.2003
- Règlement n° 2002-13 relatif à la monnaie électronique /Journal Officiel de la République Française

CESAG - BIBLIOTHEQUE

établissements de crédit qui sont régis par la loi bancaire, et compétents dans le domaine ;

4- Les droits et les obligations s'imposant aux participants respectifs d'un système de monnaie électronique doivent clairement être définis et transparents ;

5- Les systèmes de monnaie électronique doivent établir des garanties adéquates sur le plan technique, opérationnel et procédural, afin d'identifier, d'empêcher, de réduire les menaces à la sécurité du système, en particulier la menace de contrefaçon ; la protection contre l'usage illicite, tel le blanchiment d'argent, doit être prise en considération au moment de la définition et la mise en place du système de monnaie électronique ;

6- Les acteurs intervenant dans l'émission de la monnaie électronique, doivent fournir à la banque centrale toute information susceptible d'intéresser les objectifs de la politique monétaire ;

7- Les émetteurs de monnaie électronique, doivent également être à mesure de rembourser à sa valeur nominale, la monnaie électronique en monnaie Banque Centrale à la demande du porteur sous forme de monnaie fiduciaire ou de virement ;

8- Le contrat régissant l'émission de la monnaie électronique, doit préciser clairement les conditions de remboursement en cas de non utilisation des valeurs électroniques stockées dans le support électronique, sans que les établissements de crédit ne puisse prévoir d'autres frais que ceux strictement nécessaires à l'opération de remboursement ;

9- Ce remboursement doit être obtenu en cas de perte ou de vol, destruction ou défaut technique du support de la monnaie électronique, sous réserve que la valeur de la monnaie électronique soit techniquement déterminable ;

10- Les fonds remis contre la monnaie électronique ne peuvent être inférieurs à la valeur monétaire représentant la créance sur l'émetteur ;

CESAG - BIBLIOTHEQUE

11- La valeur des unités de monnaie électronique incorporées dans un support électronique (PME) émis par les établissements bancaires et financiers, ne peut excéder à aucun moment 100.000 FCFA ;

12- Le capital minimum de l'Institut d'émission de valeurs électroniques (EVUMOA), doit être fixé à 1.000.000.000 FCFA. Ce capital doit être intégralement souscrit et libéré ;

13- Les fonds propres de l'EVUMOA ne peuvent devenir inférieurs au montant du capital exigé. S'ils venaient à diminuer, les autorités de contrôle peuvent accorder un délai limité pour que l'établissement régularise sa situation ou cesse ses activités ;

14- Conformément aux directives de la Banque des Règlements Internationaux (BRI), les fonds propres des établissement de monnaie électronique doivent être à tout moment égaux ou supérieurs à 2% du montant quotidien des engagements financiers correspondant aux dettes représentatives de la monnaie électronique ;

15- Les activités commerciales d'un établissement de monnaie électronique autre que l'émission de la monnaie électronique sont limitées :

- A la fourniture de services financiers étroitement liés à l'émission de la monnaie électronique, telle que la gestion de la monnaie électronique ;

- Au stockage de données sur le support électronique pour le compte d'autres entreprises ou institutions publiques ;

16- Les établissements de monnaie électronique ne peuvent détenir aucune participation dans une entreprise, sauf si celle-ci exerce des fonctions liées à la monnaie électronique émise ou distribué par l'établissement concerné ;

17- Dans un souci d'éviter l'émission de monnaie électronique en volume élevé et de façon incontrôlée, la BCEAO doit imposer à tous les établissements oeuvrant dans ce domaine, de constituer des réserves obligatoires ;

18- Les autorités de contrôle doivent vérifier de manière stricte et permanente la liquidité et la solvabilité des établissements de monnaie électronique ;

CESAG - BIBLIOTHEQUE

19- L'EVUMOA et les établissements de crédit émettant des PME, doivent mettre en place un système automatisé de surveillance des transactions inhabituelles ayant comme support la monnaie électronique.

Les banques, les établissements financiers et les SFD doivent communiquer à l'EVUMOA toutes les anomalies constatées ayant un lien avec la circulation de la monnaie électronique. L'Institut d'émission de monnaie électronique peut prendre des dispositions visant à s'assurer que les établissements de crédit distributeurs appliquent les normes de sécurité et de vigilance définies.

CESAG - BIBLIOTHEQUE

L'Afrique en général et l'UEMOA en particulier est en train d'aborder un tournant décisif de son histoire. En effet longtemps montrée du doigt et marginalisée sur l'échiquier mondial, à cause de son système bancaire et financier vétuste et très mal sécurisé, elle est en train d'émerger petit à petit grâce à la réforme de ses systèmes et moyens de paiement, entreprise par la Banque Centrale des Etats de l'Afrique de l'Ouest, et mise en place grâce à l'appui des partenaires étrangers.

Ainsi nous avons vu au travers de notre étude, que la zone UEMOA était sous bancarisée avec un taux de bancarisation compris entre 9 et 10%. Au 28 juillet 2004, le nombre de banques agréées par les autorités monétaires était de 74 contre 24 pour les établissements financiers. Un nombre dérisoire comparé à toute à la population de l'union estimée à 74.3 millions d'habitants. Les principaux instruments scripturaux utilisés dans la zone sont le chèque, la carte bancaire, les effets de commerce, le virement et le prélèvement automatique. La carte bancaire présente quelques risques de fraudes, essentiellement dues à l'usage de la piste magnétique jugée peu fiable. Mais avec l'avènement des cartes de nouvelle génération (à microprocesseur), les transactions seront plus sécurisées et les cartes infalsifiables. La biométrie associée au système interbancaire de transaction par carte est aussi une des solutions préconisées. Quant aux chèques et effets de commerce, nous notons leur migration vers la dématérialisation avec l'échange d'images scannées ; ce qui réduit considérablement les risques de fraude, occasionnés par la manipulation physique des vignettes, ainsi que le délai de paiement.

Le paysage bancaire de l'UEMOA en pleine mutation, est sur le point d'adopter le porte monnaie électronique via les cartes multiapplicatives, permettant des paiements de petits montants. Mais face à une technologie de plus en plus complexe et de ce fait difficile à maîtriser, de nombreux risques subsistent, quant à la protection des consommateurs, des commerçants et aussi à la fiabilité et stabilité financière des établissements émetteurs de monnaie et de porte-monnaie électronique. Ainsi, une réglementation prudentielle bien appropriée, ni trop rigide, ni trop laxiste, permettrait de bien délimiter les champs d'action des participants et définir les droits et devoirs des acteurs intervenant dans le système de monnaie électronique.

Cette réforme des systèmes et moyens de paiement va permettre aux pays de l'UEMOA de faire face à cette «nébuleuse» que constitue la menace d'un risque systémique essentiellement liée aux fraudes bancaires ainsi qu'à la falsification des moyens de paiement scripturaux.

En apportant plus de sécurité, de fiabilité et de rapidité, le système bancaire s'offre des garanties solides, nécessaires à sa survie, lui permettant par la même occasion d'être en phase avec la mondialisation de l'économie.

CESAG - BIBLIOTHEQUE

GLOSSAIRE

CESAG - BIBLIOTHEQUE

Authentification

L'authentification est la vérification de l'identité d'une personne (ou d'un hôte : serveur et client). Cela garantit l'identité de la personne qui a signé les données - de cette façon vous savez qui a participé à une transaction et que celle-ci n'a pas été falsifiée. Cela permet de déterminer de façon irrévocable l'utilisateur qui tente d'accéder à un système grâce à la confirmation de son identité.

Biométrie

C'est une méthode d'identification du détenteur d'une carte bancaire par exemple, par reconnaissance d'une caractéristique physique unique de la personne (empreintes digitales, reconnaissance vocale ou de l'iris).

Carte à microprocesseur ou à puce

C'est une carte qui possède des capacités de calcul qui lui permette de réaliser ses propres opérations et contrôles. En outre, seul un microprocesseur doté de crypto processeur (composant électronique puissant), permet de faire des calculs cryptographiques complexes pour la réalisation du contrôle de code PIN en local, dans la carte. La carte à microprocesseur possède beaucoup d'avantage, notamment concernant la sécurité (vérification du code en local par la carte, authentification réciproque carte terminal, calcul d'un certificat de la transaction), et aussi la possibilité d'utiliser de nombreux canaux de communication pour effectuer des paiements (Internet, téléphone portable, télévision «pay-per-view»).

Clé

Une clé est une valeur numérique unique qui fait partie de l'algorithme de chiffrement. Il s'agit d'une suite de caractères utilisée pour coder et décoder un dossier. La clé est utilisée pour chiffrer et déchiffrer un message. Pour la cryptographie de «clés symétriques», la même clé est utilisée pour chiffrer et déchiffrer le message. Pour la cryptographie «clé publique» la clé publique est utilisée pour chiffrer le message, alors que la clé privée est utilisée pour le déchiffrer.

Certificat numérique

Un certificat numérique permet de vérifier que quelqu'un a bien le droit d'utiliser une clé, aidant ainsi à éviter qu'une personne utilise une fausse clé pour se faire passer pour quelqu'un d'autre.

CESAG BIBLIOTHEQUE

CMC7 : Caractère Magnétique Codés à 7 bâtonnets

Le marquage est effectué sur la bande réservée à l'impression des caractères magnétiques situées en bas du chèque et sur toute sa longueur, aux moyens des caractères dits CMC7 (Caractères Magnétiques Codés à 7 bâtonnets).

Compensation automatisée

C'est un système de compensation électronique, à travers lequel des ordres de paiement sont échangés entre les institutions bancaires et financières, par le canal de support magnétique ou de réseaux de télécommunication.

Création et vérification d'une signature électronique

Pour créer une signature électronique, le signataire crée un hash (empreinte numérique), condensé unique du message et utilise ensuite sa clé privée pour chiffrer ce hash. Ce hash chiffré est la signature électronique. Si le message est ensuite altéré, le hash qui en résulterait serait différend.

Si les deux hash correspondent, deux choses ont été vérifiées :

- La signature électronique a été créée en utilisant la clé privée du signataire (assurance que la clé publique correspond à la clé privée de l'expéditeur). Personne ne se fait passer pour le signataire.

- L'authenticité du signataire est vérifiée et le signataire ne peut nier avoir envoyé le message ;

- Le message n'a pas été altéré. L'intégrité du message est vérifiée.

Cryptographie

La cryptographie est l'art de transformer des informations lisibles (texte) en des informations que seules les personnes autorisées peuvent lire. Au cours de ce processus, l'information est codée (chiffrée) de façon à ce que seul le destinataire puisse lire ou altérer le message. Il peut être intercepté mais n'est intelligible que pour la personne qui est capable de le décoder (déchiffrer). Le chiffrement et le déchiffrement nécessitent une formule mathématique (ou algorithme) pour convertir les données lisibles en un format codé et une clé. Une clé est un nombre unique, combiné avec du texte pour produire un message chiffré ou une signature électronique.

CESAG - BIBLIOTHEQUE

Cryptographie asymétrique

Ensemble de techniques cryptographiques qui utilise 2 types de clés (privée et publique), pour crypter ou décrypter des données.

Digicash

C'est une entreprise américaine crée par David Chaum. Son but était de permettre aux «cyberconsommateurs» de disposer d'une enveloppe d'argent électronique et ce à partir de leur compte bancaire pour effectuer des transaction en ligne. L'opération met en oeuvre trois parties : le client, la banque et le commerçant. Ceux-ci doivent disposer des logiciels adéquats et se tenir prêt à accepter cette forme de paiement. Le logiciel gère les pièces que le client possède sur son disque dur. Lorsque le client veut retirer de l'argent électronique de son compte bancaire, son logiciel Digicash envoie à sa banque un code qui constitue une sorte de pièce "vierge". Le code est caché dans une "enveloppe" digitale. La banque vérifie que le compte est créditeur et oppose sa signature électronique sur l'enveloppe qui confère à la pièce sa valeur monétaire. L'avantage de cette monnaie est l'anonymat mais son inconvénient est dans le fait que le client ne peut effectuer ses achats qu'à partir de son propre ordinateur puisque le programme gérant le Digicash se trouve dans le disque dur de son ordinateur.

Intégrité et confidentialité des données dans un e-mail signé numériquement

La signature électronique protège l'intégrité des données. Cela signifie que vous savez que le message que vous lisez n'a pas été altéré, volontairement ou involontairement. D'un point de vue technique, la signature électronique contient un hash (empreinte numérique) de l'ensemble du message qui a été signé. Toute modification apportée à ce document après signature rend ce hash invalide.

Monnaie scripturale

«La monnaie scripturale est une monnaie sur support papier ou électronique admis par le règlement portant adoption d'un dispositif juridique sur les systèmes de paiement dans les Etats membres de l'UEMOA comme moyens de paiement valable»[19].

Elle est composée des dépôts à vue ouverts auprès des établissements de crédit (les banques), de la Poste, des Caisses nationales d'épargne, du Trésor public. Elle est créée et transférée d'un compte à un autre par un simple jeu d'écriture. Il ne faut pas confondre la monnaie scripturale (les fonds déposés) et les instruments qui permettent sa circulation comme les chèques, le virement, les cartes de paiement qui sont les instruments de règlements. La monnaie scripturale est donc la monnaie détenue par les agents sur leurs comptes

[19] Source : directives N°08/2002/CM/UEMOA

CESAG - BIBLIOTHEQUE

bancaires, c'est-à-dire, non seulement les dépôts à vue sur les comptes courants, mais aussi les dépôts sur les autres comptes (livrets, comptes à terme...).

Monnaie électronique

Selon la définition de la Banque de Règlements Internationaux (BRI), «la monnaie électronique est une valeur monétaire mesurée en unités fiduciaires et stockée sous forme électronique dans une puce électronique détenue par le consommateur»[20]. Il s'agit donc d'une forme de monnaie scripturale, stockée sur un support amovible du type carte à puce.

Porte monnaie électronique

Le porte monnaie électronique permet d'effectuer de paiements de petits montants à partir d'une réserve de fonds préalablement constituée et matérialisée par une carte. Cette réserve étant débitée par le commerçant à chaque achat. Les unités de paiement contenues dans ces cartes (logiciels) sont achetées soit directement avec la monnaie fiduciaire, soit par le débit d'un compte bancaire.

Monnaie virtuelle

La monnaie virtuelle se distingue de la monnaie électronique par le fait que son support, sa présentation et son mode de paiement n'ont pas de formes tangibles. La monnaie virtuelle peut être contenue dans des logiciels qui permettent d'effectuer des paiements sur des réseaux ouverts, en l'occurrence Internet.

Comme la monnaie électronique, la monnaie virtuelle est reliée aussi à un compte bancaire. La valeur n'est donc jamais détenue physiquement par le porteur.

La monnaie virtuelle peut être un jeton virtuel émis par un émetteur de confiance pour un usage unique et circulant dans un circuit clos. Ces jetons se distinguent des versions électroniques parce qu'ils sont uniquement reconnus dans un circuit commercial fermé.

Monnaie numérique

La monnaie numérique, est une solution ambitieuse pour les systèmes de paiement en ligne. Il s'agit en effet de créer une monnaie parfaitement adaptée à la vitesse et à l'omniprésence des réseaux informatiques tout en préservant les propriétés de la monnaie fiduciaire classique (respect de la vie privée, anonymat et difficulté de contrefaçon). Ce qui distingue la monnaie numérique de la monnaie classique est que son support est complément « virtuel » : la valeur est stockée sous forme d'algorithmes en mémoire d'ordinateur, sur le disque dur de l'utilisateur ou dans une carte à microprocesseur.

[20] Source : site Internet BRI

CESAG - BIBLIOTHEQUE

La banque du système échange la monnaie numérique contre de la monnaie physique après avoir consulté une base de données de vérification, qui peut être centralisée ou distribuée. L'échange de valeurs entre les différentes parties d'une transaction se fait en temps réel via le réseau, mais la compensation financière avec la banque se déroule soit en temps réel, soit en différé.

A l'instar de la monnaie physique, la monnaie numérique permet de dissocier le billet de paiement de l'identité du porteur, afin de rendre les transactions complètement anonymes. C'est en cela qu'elle se distingue des autres monnaies électroniques.

CESAG - BIBLIOTHEQUE

Monétique

Contraction de **moné**(taire) et d'(informa)**tique**, désigne l'ensemble des techniques électroniques, informatiques et télématiques permettant d'effectuer des transactions, des transferts de fonds (carte bancaire, virement électronique,..).

Non répudiation d'un e-mail signé numériquement

L'auteur (la personne qui signe) d'un message prouve son identité. La non répudiation établit plus tard, qui a participé à une transaction. L'expéditeur ne peut nier avoir envoyé le message et le destinataire ne peut nier l'avoir reçu. Simplement la non répudiation signifie qu'une information ne peut être rejetée, tout comme avec les signatures manuscrites.

Normes EMV : (Europay MasterCard Visa)

Les normes EMV définissent le nouvel environnement pour les transactions par carte bancaire en mettant en place de nouveaux standards (logiciels, terminaux). Ces normes reposent sur la technologie puce.

Les spécifications EMV, définies au cours des dernières années, sont constituées de règles qui garantissent l'interopérabilité globale entre les cartes à puces et les terminaux de paiement, indépendamment des constructeurs, des banques émettrices de cartes ou lieu de paiement. A cet effet, un processus d'homologation des terminaux de paiement a été mis en place, afin de contrôler, par des tests, la conformité des terminaux à la norme EMV.

Reconnu dans de nombreux pays, le standard EMV offre un très haut niveau de sécurité.

Protocole 3D Secure

Voici le déroulement d'une transaction selon le protocole 3D Secure :

1- Le porteur de carte remplit son bon de commande et fournit son numéro de carte bancaire à son commerçant. Il reçoit alors de la part de sa banque un message lui demandant de s'authentifier.

2- Le commerçant demande l'authentification du porteur de la carte. Il utilise alors le numéro de carte et le transmet au service *Verified by visa* (VbyV).

3- La banque émettrice vérifie que le numéro correspond à un porteur inscrit au service VbyV.

4- La banque émettrice authentifie le porteur

5- La banque envoie la preuve de cette authentification au marchand. Le marchand poursuit alors la transaction en effectuant une demande d'autorisation auprès de la banque acquéreur.

La clé du système repose sur l'authentification de l'internaute au moment de la transaction. *Verified by Visa* protège le porteur et le commerçant affiliés au programme *Verified by visa.* Le commerçant est assuré d'être payé, même en cas de contestation de la part du porteur de carte. Il doit à cet effet installer un logiciel 3D Secure sur son site web. L'internaute y trouve également son intérêt. En réduisant le risque de fraude à la source, il fait l'économie de démarches souvent fastidieuses entraînant de longs délais de remboursement.

Signature électronique

Tout comme les signatures manuscrites, les signatures électroniques sont utilisées pour identifier les auteurs/co-signataires de données électroniques. Les signatures électroniques sont créées et vérifiées grâce aux certificats numériques. A l'heure actuelle, la communauté légale internationale élabore une législation qui reconnaîtra et donnera une valeur légale aux signatures électroniques, leur donnant la même valeur que les signatures manuscrites. Pour signer des informations, pour opérer des transactions de façon sécurisée, vous devez avoir votre propre et unique certificat numérique.

Signature RSA : (Rivest, Shamir, Adleman)

Une fois introduite dans le terminal de paiement, la carte doit s'authentifier par une signature RSA, inscrite sur la puce. Cette signature comporte quatre vingt seize (96) chiffres, et de ce fait identifie de façon unique la carte. Sa reproduction est quasiment impossible.

CESAG BIBLIOTHEQUE

Swift: Society for Worldwide Interbank Financial Telecommunications

Réseau mondial de télécommunication du secteur financier lancé en 1977. Hautement sécurisé, disponible 24h sur 24, 7jours su 7, il assure les services de transmission de messages normalisés entre les différents acteurs du monde de la finance.

CESAG - BIBLIOTHEQUE

ANNEXES

CESAG - BIBLIOTHEQUE

<u>Système Interbancaire de Compensation Automatisé de l'UEMOA</u> : SICA – UEMOA

C'est un système d'échange d'opérations de paiement automatisé qui assure la compensation multilatérale des transactions entre les participants. Il assure :

- la compensation multilatérale des transactions entre les participants ;
- l'échange d'instruments dématérialisés;
- la réduction des délais et coûts des échanges interbancaires ;
- le respect du délai maximum de règlement sur le compte de la clientèle.

Les instruments admis à la compensation sont :

- Tous les types d'instruments scripturaux en vigueur ;
- valeurs NATIONALES sur place, déplacées et hors place dans tous les Points d 'Accès à la Compensation (PACs) ;
- valeurs SOUS-REGIONALES.

les Participants sont:

- les banques commerciales;
- la Poste;
- la Banque Centrale.

les Fonctionnalités sont:

- Gestion de la participation ;
- Organisation de la journée de compensation ;
- Contrôles effectués sur une Remise Aller ;
- Gestion du règlement : intégration avec STAR-UEMOA ;
- Gestion des incidents de paiement : intégration avec la CIP.

CESAG - BIBLIOTHEQUE

Système interbancaire régional de paiement par cartes

La monétique interbancaire est caractérisée par la mise en place de deux structures interbancaires :

- Le Groupement Interbancaire Monétique (GIM-UEMOA) ;
- Le Centre de Traitement Monétique (CTM).

Le GIM-UEMOA assure les fonctions dites de gouvernance :

- Organisation de l'interbancarité ;
- Elaboration des règles et procédures interbancaires ;
- Pilotage du système monétique interbancaire et de son interopérabilité, aux plans administratif, juridique et technique ;
- Elaboration de la politique sécuritaire du système et suivi de son application ;
- Gestion de la fraude.

Le CTM assure quant à lui les fonctions dites de traitement regroupant :

des fonctionnalités obligatoires:

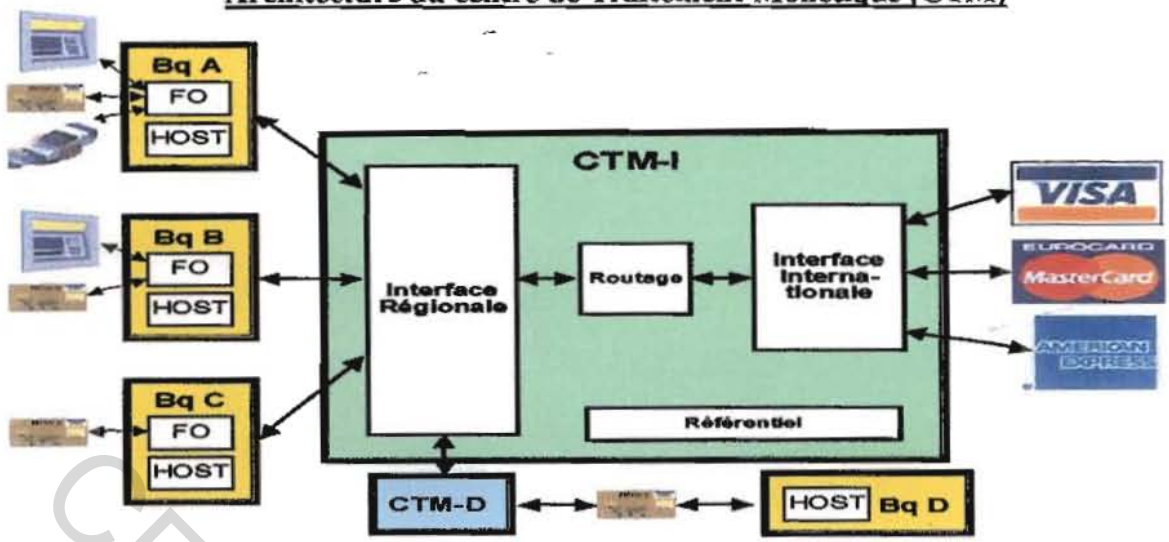
- Gestion du réseau de routage ;
- Autorisation ;
- Centre d'appels vocaux ;
- Calcul et gestion des commissions ;
- Pré-compensation.

des fonctionnalités optionnelles :

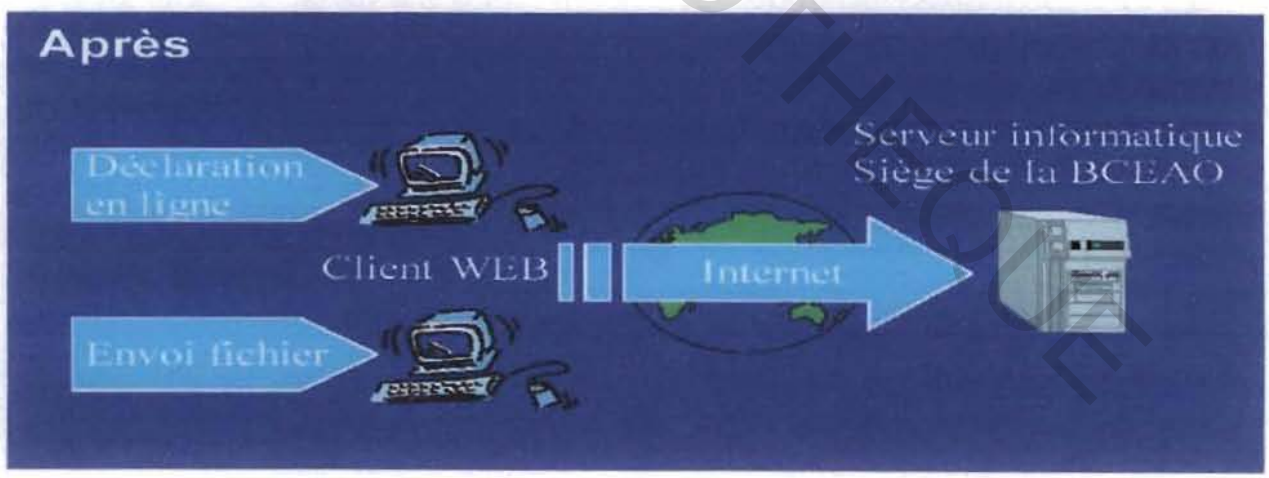
- Gestion des transactions «porteurs» ;
- Gestion des transactions «commerçants» ;
- Télésurveillance des DAB/GAB ;
- Centrale d'achat ;
- Fabrication et personnalisation des cartes ;
- Délivrance d'autorisation par délégation ;
- Interchange international.

CESAG - BIBLIOTHEQUE

Architecture du centre de Traitement Monétique (CTM)



Centrale des Incidents de Paiement : CIP



Elle permet la gestion des :

- décisions de retraits de cartes bancaires ;
- régularisations d'incidents de paiement ;
- ouvertures et clôtures de comptes sur lesquels des formules de chèques ont été délivrées ;
- oppositions pour perte ou vol ;

CESAG - BIBLIOTHEQUE

- ouvertures et clôtures de comptes sur lesquels des formules de chèques ont été délivrées ;
- oppositions pour perte ou vol ;
- faux chèques et fausses cartes ;
- refus de paiement de chèques et d'effets de commerce pour défaut de provision suffisante ou tirage sur comptes clôturés.

Les participants sont :

- les banques ;
- le parquet communique à la BCEAO les interdictions d'émettre des chèques ainsi que les suspensions et levées d'interdictions d'émettre des chèques prononcées par le Tribunal ;
- la Banque Centrale est chargée de centraliser et de diffuser toutes les informations déclarées relatives aux incidents de paiement ;
- le public.

<u>Système de Traitement Automatisé et de Règlement</u> : STAR UEMOA

Le Système STAR-UEMOA permet de :

- traiter les opérations d'importance systémique avec rapidité et en conformité avec les normes internationales;
- réduire les risques de paiement;
- faciliter la gestion monétaire et le fonctionnement du marché financier;
- faire des échanges au niveau sous régional.

Il existe 3 types de participants admis par le système :

- Direct ;
- Indirect ;
- Sous-participant.

Les participants éligibles sont :

- les banques et établissements financiers;
- la BCEAO (chaque Agence Principale et le Siège);
- les Sociétés de Gestion et d'Intermédiation boursière pour les opérations de la Bourse;

CESAG - BIBLIOTHEQUE

- le Dépositaire Central/Banque de Règlement;
- d'autres institutions financières sous-régionales faisant l'objet d'une dérogation (BOAD, Structures de Micro-Finance, etc.…).

Les Opérations traitées dans STAR-UEMOA sont celles interbancaires (virements en francs CFA entre participants, règlement/livraison des titres conservés en Banque Centrale, règlement des opérations de pensions livrées, règlement des espèces pour les opérations de la BRVM) et celles propres à la Banque Centrale (retraits et dépôts fiduciaires, règlement des soldes de compensation, règlements des opérations de Politique Monétaire et de la dette publique, couverture en francs CFA des opérations de transferts internationaux).

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

OUVRAGES – REVUES

- « Intelligence artificielle, la Biométrie », FIAT Bastien, GIRARD Jean-Patrick, LARRE Bruce, MALGRAS Antoine : 11 avril 2003.

- « Les moyens de paiement : des espèces à la monnaie électronique », DRAGON Claude, GEIBEN Didier, KAPLAN Daniel, NALLARD Gilbert. - Paris : la Revue Banque, 504p, 1998.

- « La monétique » - Paris : Eurostaf, 1997. - 2 vol. (63-130p.).

- « Net economy et e-business », réinventez votre système d'information autour d'Internet DALLOZ Xavier ; SALZMAN Claude ; Edition DUNOD.

- « Internet et commerce électronique », BROCHURBERG Lionel ; édition DUNOD.

- « Le porte-monnaie électronique et le porte-monnaie virtuel », SABATIER Guy - Paris : Presses Universitaires de France, 1997 - 128 p.

- « Commerce électronique et moyens de paiement », FARAGGI Benjamin. - Paris : Dunod, 1998. - 199 p.

- « Comment organiser et sécuriser le paiement électronique », L'Internet et la vente / Pôle universitaire Léonard de Vinci. - Paris : Ed. d'Organisation, 1997. - 168 p.

- « Les enjeux de la monnaie électronique », SALZMAN Claude. - Problèmes Economiques, n° 2524, 1997, p. 20.

ARTICLES - ETUDES : BCEAO/DSP/UEMOA

- Règlement n° 15 /2002/CM/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'UEMOA.

- Projet de réforme des systèmes et moyens de paiement dans les pays de l'UEMOA : système interbancaire régional de paiement par carte/BCEAO/MRMSP.

CESAG - BIBLIOTHEQUE

- Présentation du Projet CIP (Centralisation des Incidents de Paiement), par l'équipe Projet CIP, BCEAO, 03 juillet 2003.

- Etude de faisabilité d'un porte monnaie électronique, rapport final 24 juillet 2001 ; DSP-BCEAO.

- Directives n° 08/2002/CM/UEMOA.

- Télécompensation et Echanges Images Scannées, Plénière Etat des lieux du 12/03/2004 – BCEAO/DSP.

- Présentation des systèmes et moyens de paiement dans les pays de l'UEMOA, séminaire organisé par la Banque des Règlements Internationaux pour le Master en Banque et Finance du CESAG ; KWASSI Bwaki – Direction des Systèmes de Paiement/BCEAO-Siège, Février 2004.

SITES INTERNET

- « Zoom sur l'échange d'images chèques » www.bceao.int/internet.nsf/french.tm.

- « Assurer la sécurité de chaque moyen de paiement » Actualité Bancaire n° 489 29/04/2004, publication bimensuelle de la fédération bancaire française, www.fbf.fr.

- Arrêté du 10 janvier 2003 portant homologation du règlement n° 2002-13 du comité de la réglementation bancaire et financière n° 2002-13 relatif à la monnaie électronique et aux établissements de monnaie électronique, Jo, 1er février 2003, P.2003, www.droit-tecnologie.org.

- « La biométrie », www.securiteinfo.com/conseils/biomerie.shtml .

- « Le livre blanc de la signature électronique », groupe de travail du club csa, BENSOUSSAN Alain, COPIN Charles, DEPADT Marion, éditions Analyses et synthèses, novembre 1999, www.cardsow.com/clubcsa/upload/ibse.pdf .

CESAG - BIBLIOTHEQUE