CESAG **Centre Africain d'études Supérieures en Gestion**

CESAG BF – CCA
BANQUE, FINANCE, COMPTABILITE, CONTROLE & AUDIT

Master Professionnel
en Audit et Contrôle de Gestion
(MPACG)

Promotion 5
(2010-2012)

Mémoire de fin d'étude

THEME

ANALYSE DU FONCTIONNEMENT DU CENTRE DES SERVICES MUTUALISES MONETIQUE DE LA SOCIETE GENERALE (CSM M)

Présenté par :
M. Malick SENE

Dirigé par :
M. Philippe LERMUSIAUX
DIRECTEUR DU CSM M

Octobre 2012

DEDICACE

Je dédie ce mémoire à mes parents car rien ne vaut les efforts fournis et les sacrifices consentis pour mon éducation en espérant répondre un jour aux espoirs fondés en moi.

REMERCIEMENTS

Je remercie très sincèrement :

- mon épouse pour la joie qu'elle me procure, pour ses précieux conseils et son aide à la réalisation de ce travail ;

- M. Philippe Lermusiaux, Directeur du CSMM, qui a accepté d'être mon directeur de mémoire, qui m'a fourni toutes les informations dont j'avais besoin et qui par-dessus tout m'a donné l'opportunité d'intégrer le CSMM ;

- le corps professoral et l'ensemble du personnel du CESAG pour la qualité de la formation ;

- ma famille, ma belle famille, mes amis proches pour avoir d'une manière ou d'une autre apporté leur contribution à la réalisation de ce mémoire.

LISTE DES SIGLES ET ABREVIATIONS

AFFN : Armed Forces Financial Network

AMEX: American Express

ANSI: American National Standards Institute

BCEAO : Banque Centrale des Etats de l'Afrique de l'Ouest

BHFM : Banque Hors France Métropolitaine

BIN: Bank Identification Number

BOM: Back Office Monétique

BSI : British Standards Institution

CENB : Comité Européen de Normalisation Bancaire

CESAG : Centre Africain d'Etudes Supérieures en Gestion

CIE : Commission Internationale électronique

CNN Comités Nationaux de Normalisation

CSM : Centre des Services Mutualisés

CSMCR : Centre des Services Mutualisés Comptabilité Reporting

CSMM : Centre des Services Mutualisés Monétique

CSMSI : Centre des Services Mutualisés Système d'information

CUP: China Union Pay

DAB : Distributeur Automatique de Billet

EME Les établissements de monnaie électronique

EMV: Europay Mastercard Visa

GAB : Guichet Automatique Bancaire

GIM-UEMOA : Groupement Interbancaire Monétique de l'Union Economique et Monétaire Ouest Africaine

IETF: Internet Engineering Task Force

ISO: International Organization for Standardization

JCB: Japan Credit Bureau

KPI: Key Performance Indicator

NCR: National Cash Register

OCDE: Organisation de Coopération et de Développement Economique

PAN: Personal Authentication Number

PCI: Payment Card Industry

PCI – PA: Payment Card Industry Payment Application

PCI-DSS: Payment Card Industry - Data Security Standard

PCI-PED: Payment Card Industry - PIN Entry Device

PCI-SSC: Payment Card Industry - Security Standards Council,

PIN: Personal Identification Number

PNB : Produit Net Bancaire

PTS : PIN Transaction Security

RIB Relevés d'Identité Bancaire

SG: Société Générale

SGBS : Société Générale de Banques au Sénégal

SLA : Service-Level Agreement

TPE: Terminal de Paiement Electronique

UEMOA: Union Economique et Monétaire Ouest Africaine

UIT : Union Internationale des Télécommunications

UMOA : Union Monétaire Ouest Africaine

LISTE DES TABLEAUX ET FIGURES

Liste des tableaux

Liste des figures

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

En observant bien le monde de la finance de nos jours, nous remarquons 4 tendances que sont le regroupement des institutions, l'universalisation des opérations, le développement des nouvelles technologies et la mondialisation des activités bancaires. L'importance, l'influence et la place qu'occupent les banques sont de plus en plus grandissantes. Selon BCEAO (2012 :2) « les pays développés ont un taux de bancarisation d'au moins 90% et l'Afrique reste en gros le dernier marché bancaire à conquérir avec des taux variant entre 10 et 30% selon les pays. Par exemple, le taux est de 15% pour les pays de l'Union Economique et Monétaire Ouest Africaine (UEMOA) ». La population adulte d'Afrique Subsaharienne non bancarisée reste donc très élevée par rapport à celle des pays de l'Organisation de Coopération et de Développement Economiques (OCDE) à revenus élevés.

Au Sénégal, le système bancaire était constitué initialement de banques françaises. L'Etat a ensuite contribué à la mise en place d'un nouveau système. Mais face à la crise de liquidité des années 80 due à une mauvaise gestion, la restructuration fut décidée permettant entre autre de réduire l'implication de l'Etat. De nos jours, le nombre de banques et d'établissements financiers est en constante progression au Sénégal (20 banques et 4 établissements financiers) avec une forte présence de firmes étrangères. Les banques sont de plus en plus compétitives et misent sur la conception et la vulgarisation de produits bancaires adaptés.

La création de structures comme le Centre des Services Mutualisés Monétique (CSMM) répond au besoin de deux tendances que sont l'économie d'échelle et le développement de la monétique. D'une part, les initiatives s'apparentant à une mutualisation, à la mise en commun des ressources et des moyens se développent de plus en plus pour permettre une économie d'échelle et aussi favoriser l'innovation. D'autre part nous remarquons de plus en plus un développement progressif de la monétique. En permettant de moderniser les moyens de paiement qui sont des instruments utilisés pour transférer des fonds à travers des supports et méthodes variés, la monétique dynamise le système bancaire. C'est un ensemble de techniques informatiques et électroniques de gestion des cartes bancaires. OTMAN (1998 : 244) définit la monétique comme l'«ensemble des technologies associant l'informatique et les transactions monétaires ». Elle bénéficie de l'appui de la BCEAO qui soutient l'interbancarité afin de vulgariser l'utilisation de la carte bancaire et aider au développement de la monétique dans l'UEMOA et au Sénégal. C'est pourquoi lors dans la réforme des systèmes de paiement de la BCEAO, un volet monétique a été spécialement pris en compte. Les orientations stratégiques de ce volet visent particulièrement :

- la mise en place d'une interbancarité régionale à travers l'interopérabilité des GAB ;
- l'institution d'une carte bancaire de retrait et/ou de paiement utilisable dans toute l'UEMOA et hors de l'UEMOA ;
- l'utilisation de la technologie fondée sur la puce aux normes Europay Mastercard Visa (EMV) afin de renforcer la sécurité des transactions.

Les banques peuvent aussi bénéficier d'une interconnexion plus large à l'échelle internationale en adhérant à des réseaux internationaux comme Visa, Mastercard, American Express, etc. La monétique ne se limite pas seulement au fonctionnement de la carte bancaire mais elle prend aussi en compte les extensions telles que le porte-monnaie électronique, le paiement par téléphone mobile, les transactions associées à la carte bancaire, etc.

Le Centre des Services Mutualisés Monétique (CSMM) a été mis en place à Dakar par le groupe Société Générale en mars 2010 pour regrouper et gérer la fonction monétique de ses 10 filiales d'Afrique subsaharienne en créant un pôle d'expertise monétique. Depuis 2012, un second centre a ouvert ses portes à Antananarivo (Madagascar).

Pour atteindre ses missions telles que la création d'un pôle d'expertise et la mise en place de services monétiques de qualité, mais aussi pour être en adéquation le projet de la Société Générale nommé « ambition SG 2015 » ayant pour principal objectif la croissance au moindre risque, le CSMM se doit de respecter certaines normes et référentiels. Ces normes et référentiels qui ne sont sans doute pas toujours respectés rentrent aussi bien dans le cadre de son activité qu'est la monétique que dans son mode de fonctionnement.

La monétique est une activité risquée. En tant que moyen de paiement, la carte bancaire, outil principal de la monétique est très vulnérable et fait souvent l'objet de fraude. Cette situation fait que le secteur de la monétique fait l'objet d'une réglementation stricte et est régi par de nombreuses normes et réglementations. De plus, en tant que entité d'un grand groupe bancaire, avec une activité qui ne cesse de grandir et d'évoluer, le CSMM fait face à des exigences auxquelles elle doit forcément se soumettre. L'équipe dirigeante et les agents cherchent donc à constamment s'adapter, s'organiser, évoluer, innover pour se mettre à niveau des attentes. La structure fait face à des filiales et à une maison mère qui sont de plus en plus exigeantes avec une pression permanente d'autant plus que les sanctions couru en cas

de non respect des normes de même que la vulnérabilité à laquelle il s'expose risquent d'avoir une répercussion sur l'ensemble des filiales.

Les solutions possibles pour faire face à ce problème sont entre autres :

- la connaissance des normes qui régissent l'activité du CSMM ;
- l'élaboration d'un plan d'action et des manuels de procédures pour la pour la mise en conformité avec les exigences du moment ;
- l'analyse du fonctionnement du centre pour s'assurer de l'application des dites normes;

Pour répondre de manière plus adéquate à la problématique, une analyse doit d'abord être faite en guise d'évaluation pour connaitre la situation actuelle. De ce fait, la solution la plus logique et que nous avons retenue est d'identifier les principales normes monétiques, les plus importantes, et de vérifier leur niveau d'application.

La question principale qui se pose à nous est : Comment analyser et évaluer le fonctionnement du Centre des Services Mutualisés Monétique de la Société Générale ?

Cette question principale en appelle d'autres plus spécifiques que sont :

- qu'est-ce que la monétique ?
- quelles sont les principales normes en matière de monétique ?
- comment fonctionne le CSMM ?
- que fait le CSMM pour être en adéquation avec ces normes?
- quels sont les risques que connaît le CSMM-SG ?

Nous répondrons à ces questions à travers ce mémoire dont le thème est : « Analyse du Fonctionnement du Centre des Services Mutualisés Monétique de la Société Générale ».

L'objectif principal est d'analyser le fonctionnement de la CSMM et de voir si les normes sont respectées au sein du CSMM et si oui à quel point.

Les objectifs spécifiques sont :

- comprendre l'activité du CSMM ;
- connaître les principales normes qui réglementent cette activité ;

- évaluer le niveau d'application des normes ;
- formuler des recommandations pour un meilleur fonctionnement et une meilleure prise en compte de celles-ci.

Nous ne pourrons pas dans ce mémoire évoquer en profondeur toutes les normes de la monétique, cependant nous nous limiterons aux normes de sécurité PCI DSS pour les données de cartes au niveau des GAB (Guichet automatique bancaire). PCI-DSS est un ensemble homogène de normes de sécurité pour la gestion des données de carte valables dans le monde entier. Les directives qui y sont définies s'appliquent à toutes les parties (commerçants, Acquéreurs, Service Providers etc.) qui transmettent, traitent et/ou stockent des données de cartes.

L'intérêt du sujet est double :

- pour CSMM : il s'agira de disposer d'un document présentant ses activités et qui fait le point sur la sa situation actuelle par rapport à certaines normes qu'elle doit respecter. Elle pourra par la suite se baser sur ce document pour réagir plus efficacement concernant les actions à mener ;
- pour nous même : ce mémoire permettra de mieux maitriser l'environnement dans lequel nous travaillons, d'avoir une meilleure connaissance des normes monétiques et d'améliorer nos capacités d'analyse.

Ce mémoire comportera deux grandes parties :

- la première partie comportera trois chapitres. Le premier chapitre parlera de la monétique en général, le deuxième chapitre parlera des normes monétiques et le troisième chapitre sera consacré à la méthodologie de recherche.
- dans la deuxième partie, nous ferons d'abord une présentation générale du CSMM, puis nous parlerons des activités du CSMM d'un point de vue application des normes et enfin nous ferons une analyse suivie de recommandations.

PREMIERE PARTIE : CADRE THEORIQUE

INTRODUCTION DE LA PREMIERE PARTIE

Les marchés monétiques nationaux des pays de l'UEMOA sont pour la plupart à l'état embryonnaire et caractérisés par une absence d'interbancarité et d'interopérabilité entre les systèmes existants, mais leur potentiel d'évolution pour les services monétiques est important.
Eu égard à cette carence au niveau de l'UEMOA, la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a initié, en 1999, un projet d'envergure régionale visant à la modernisation des systèmes de paiement dans les huit pays de l'UEMOA.
Cette Réforme des Systèmes de Paiement dans l'UEMOA s'inscrit notamment dans le cadre général de l'assainissement du système financier et de l'accélération du processus d'intégration économique régionale.

Pour faciliter respectivement le financement, surtout à court terme, des opérations commerciales et le paiement de sommes d'argent sans manipulation d'espèces, la pratique des affaires et particulièrement les banquiers ont mis au point des procédés appelés communément les instruments de crédit et les instruments de paiement.

La première partie comportera un premier chapitre sur la monétique, un second sur les normes monétiques et un troisième sur la méthodologie de la Recherche.

CHAPITRE 1 : LA MONETIQUE

Introduction

Lorsqu'on parle de la « monétique », il est nécessaire aujourd'hui de dissocier l'approche dite traditionnelle du domaine bancaire, c'est-à-dire en rapport avec la « monnaie électronique » et les « systèmes et moyens de paiement électroniques » de la mutation engagée depuis les années 1990 qui étend ses applications à d'autres domaines comme la santé (carte Vitale), le transport (Pass Navigo), la téléphonie mobile (carte SIM), la domotique, le commerce électronique, etc..

La difficulté actuelle de la définition du mot « monétique » et de son périmètre réside dans la limitation des domaines car la liste des services et de ses applications n'est pas exhaustive aujourd'hui. Pour exemple, on a coutume d'appeler « monéticien » le professionnel travaillant sur des sujets monétiques. Initialement, le monéticien était un expert traitant de la carte bancaire avec une approche en maitrise d'ouvrage et/ou en maitrise d'œuvre. Cependant, la carte bancaire se transforme en reposant sur des supports électroniques (exemple : « E-Carte Bleue »). Le métier du « monéticien » évolue ainsi depuis l'avènement d'Internet et de l'essor de la vente à distance afin de répondre aux questions posées par la sécurité des transactions en environnements ouverts.

1.1 Définition de la Monétique

Selon Hallépée (2010 : 14), « la monétique est un monde en perpétuelle évolution ». Elle comprend l'ensemble des technologies nécessaires à l'utilisation, à l'émission et la gestion des cartes bancaires ainsi que des transactions qui leur sont associées. Selon le même auteur, quand on parle de monétique, on fait aussi allusion :

- à la création et la personnalisation des cartes ;
- aux systèmes permettant l'usage des cartes ;
- au matériel acceptant les cartes ;
- au système de traitement des transactions autrement dit la compensation.

Selon le site internet wikipedia, la monétique désigne l'ensemble des traitements électroniques, informatiques et télématiques nécessaires à la gestion des transactions monétaires et de transferts de fond monétaires à savoir :

- dans un premier temps, la monétique a renforcé l'utilité de la monnaie scripturale et a permis la gestion dématérialisée des chèques et a rendue possible, grâce aux virements électroniques, la banque à distance. Elle est à l'origine de l'essor des cartes de paiement (carte bancaire de crédit et de débit).
- dans un second temps, la monétique a crée la monnaie électronique qui n'est plus rattachée à aucun compte de banque ou de commerçant. Elle existe par une information codée représentant une somme d'argent utilisé pour le règlement de sommes peu importantes.

Selon le Conseil Economique et Social Français, « La monétique est l`ensemble des techniques informatiques, magnétiques, électroniques et télématiques permettant l'échange de fonds sans support de papier ».

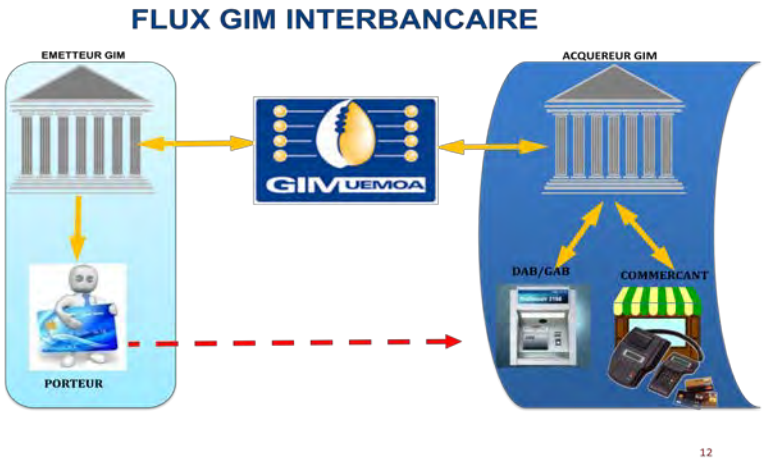
Le Larousse Economique 2003, quant à lui, définit la monétique comme « l'ensemble des moyens techniques utilisés pour automatiser les transactions bancaires et monétaires. La monétique assure notamment la gestion des cartes bancaires, la distribution automatique des billets ainsi que les systèmes électroniques de transfert d'informations ou de fonds ».
La monétique fait partie du domaine des Transactions Electroniques Sécurisées.

1.2 La gestion des flux en monétique

La gestion des flux dans le domaine de la monétique n'est possible qu'à la condition que les différents acteurs (émetteur, porteur, accepteur, acquéreur) adhérent sans réserve aux multiples contraintes imposées par les systèmes de transfert des informations proposées par les établissements financiers.

Le typage des informations obéit à des règles très strictes et normalisées au niveau international. Ces flux doivent s'accompagner d'une inviolabilité de leur contenu. Ainsi, un cryptage fort est mis en place à toutes les étapes de transfert des informations.

Figure 1 Flux GIM Interbancaire



Source : GIM-UEMOA (2006)

Selon Guntberg (2006 :32), « on distingue trois catégories de flux : internet, intranet et extranet ». Similairement à ceux présents sur la toile (Intranet, Internet et Extranet), la gestion des flux sera différente quant à sa gestion et son contenu, selon qu'il circule au sein même de l'établissement financier, entre les différents établissements financiers ou en direction des tierces parties ou des clients.

Le souci principal lié à la gestion des flux consiste à faire en sorte que seules les informations « nécessaires » à la cible concernée (collaborateur, tiers, client, agent de changes, etc.) soient mises à disposition. Au sein même de l'établissement financier, ne seront accessibles aux collaborateurs que les informations dont ils ont la charge de gestion opérationnelle.

1.3 Les acteurs de la Monétique

Selon Ordonneau (2011 :40) dans sont livre intitulée la bancarisation, « les différents intervenants lors d'une transaction monétique sont : le porteur, l'accepteur, l'émetteur, l'acquéreur » :

- le porteur : titulaire de la carte, en général le propriétaire du compte bancaire qui lui est associé, mais il peut aussi en être un simple mandataire ;
- l'accepteur : commerçant ou organisme (DAB/GAB, site internet…) qui accepte les règlements par carte bancaire. Si c'est un commerçant, il signe un contrat commerçant avec la banque acquéreur, il dispose d'un compte bancaire au niveau de cette banque, il paiera aussi des commissions par rapport au montant des transactions acceptés. Les

GAB sont eux considérés comme des accepteurs particuliers qui appartiennent à la banque acquéreur ;

- l'émetteur : c'est l'organisme financier qui émet la carte et la met à disposition du client. Il peut être un établissement financier, un établissement de paiement ou un établissement de monnaie électronique;
- l'acquéreur : c'est un organisme financier qui met à disposition des commerçants tous les services lui permettant de recevoir des paiements monétiques. Il peut être un établissement financier, un établissement de paiement ou un établissement de monnaie électronique. Il assure la gestion des GAB et des TPE.

1.4 Les équipements utilisés en Monétique

Selon Hounyonou (2006 : 18), « les équipements utilisés dans la monétique sont la carte, le point d'acceptation et le serveur » :

- la carte bancaire qui est support plastique; à piste magnétique, à puce, ou sans contact ; sur lequel sont enregistrées des informations relatives au compte sur lequel la carte est adossée, et utilisé comme moyen de paiement. Une présentation plus détaillée se fera dans la partie suivante ;
- le terminal ou point d'acceptation qui peut être un distributeur automatique de billets, un terminal de paiement électronique une borne ou un automate non bancaire (distributeur de biens ou de services). Le guichet automatique de billet est un appareil électronique et électromécanique permettant aux clients d'effectuer différentes transactions bancaires en libre service. Ces transactions peuvent être des retraits, des consultations de solde, les dépôts en liquide ou par chèque, les transferts de fonds, le changement de code PIN, etc. Nous avons aussi les Distributeurs automatiques de billets qui ressemblent aux GAB mais qui ne permettent d'effectuer que des retraits et des consultations de solde. Le Sénégal ne dispose pour l'instant que de DAB. Le second point d'acceptation le plus fréquent est le TPE. Le TPE est un appareil électronique permettant de lire les données d'une carte bancaire, d'enregistrer une transaction et de communiquer avec un serveur d'authentification à distance ;
- le serveur d'autorisation dont le rôle est de décider si une transaction peut aboutir ou non en fonction des paramètres de la transaction, de la carte et du compte associé. Il peut être hébergé par la banque propriétaire de la carte ou déléguée à un prestataire externe.

1.4.1 La carte bancaire

Dans le dictionnaire du droit privé nous avons une définition de la carte bancaire. Selon Braudo (2009 : 65) c'est « un document créé par la loi n° 91-1382 du 30 décembre 1991 qui est remis par une banque à un client titulaire de compte et qui permet à ce dernier de retirer ou de transférer des fonds au profit du fournisseur d'un bien ou d'un service ». La carte bancaire est un moyen de paiement prenant la forme d'une carte émise par un établissement de crédit et permettant à son titulaire d'effectuer des paiements et/ou des retraits ; des services connexes peuvent être associés (assurance, assistance, ...).

Une carte bancaire apparaît ainsi comme un moyen de paiement sous forme de carte plastique équipée d'une bande magnétique et/ou puce électronique permettant :

- Le paiement d'achats et prestations de services auprès de fournisseurs possédant un Terminal de Paiement Electronique (TPE) pouvant lire la carte et connecté ou non à sa banque ;
- le retrait d'espèces aux Distributeurs Automatiques de Billets (DAB) ;
- le télépaiement Internet.

La carte bancaire peut se présenter sous la forme d'une carte à piste ou d'une carte à puce. La technologie carte à puce est de plus en plus répandue car elle offre, par rapport à la carte a piste, plusieurs avantages parmi lesquels nous citerons :

- L'ajout d'un microprocesseur en plus de la piste magnétique ;
- l'accroissement la sécurité car on peut très difficilement la dupliquer ;
- la possibilité de faire cohabiter plusieurs applications sur une même carte de façon étanche et sécurisée.

Figure 2 : Recto d'une carte bancaire

Source : Source GIM-UEMOA (2007)

Le document de formation version 2-6 de la société GALITT sur la monétique bancaire nous fait une présentation de la carte bancaire. C'est donc cette référence que nous avons utilisé et essayé de synthétiser comme suit :

- le recto d'une carte comprend le numéro à 16 chiffres de la carte qui permet d'identifier votre carte, le nom du titulaire , la date d'expiration et l'hologramme destiné à rendre la carte infalsifiable ;

Figure 3 : Verso de la carte bancaire

Source : GIM-UEMOA (2007)

- le verso qui comprend toujours selon Galitt le panneau de signature, la piste magnétique et le cryptogramme visuel .

VISA, dans son document VISA FIRST (2010 :43) nous dit que : « la carte peut être une carte de débit ou une carte de crédit ».

Voici ci-dessous une petite explication :

- pour la carte de débit, le montant de la transaction est prélevé immédiatement (débit immédiat) ou à échéance mensuelle (débit différé) sur le compte associé à la carte ;
- pour la carte de crédit le titulaire du compte reçoit mensuellement la facture reprenant les opérations effectuées et peut s'en acquitter par un autre moyen de paiement. Une ligne de crédit est dans ce cas associée à la carte, le montant utilisé est par la suite débité en fonction des règles de gestion du compte définies à l'avance.

Le GIM UEMOA dans se présentation des systèmes de compensations et de règlement (2011:12) stipule que « la carte peut avoir deux caractères : elle peut être privative et n'être utilisée que sur les distributeurs et terminaux de la banque qui a émis la carte ; ou interbancaire et être utilisée sur n'importe quel terminal appartenant au même réseau. »

1.4.2 Terminal de paiement électronique (TPE)

Le document de formation version 2-6 de la société GALITT (2009 :75) définit : « un terminal de paiement électronique est un appareil électronique capable de lire les données d'une carte bancaire, d'enregistrer une transaction, et de communiquer avec un serveur d'authentification à distance ». Le Terminal de Paiement Electronique est une solution de paiement idéale. Il s'agit d'un appareil installé sur votre point de vente qui permet à votre clientèle de régler tous ses achats à l'aide d'une carte de paiement bancaire (VISA, Mastercard, etc).

Les avantages du TPE pour les commerçants peuvent prendre selon notre expérience et notre observation plusieurs aspects comme la totale garantie de paiement sur les opérations à montant élevé ; la suppression de la manipulation d'espèces ; l'acquisition de nouveaux clients (locaux et internationaux) ; les facilités de paiement ; la sécurité grâce au contrôle systématique du code pin lors des transactions commerciales.

1.4.3 Le Serveur d'authentification

Selon les dispositions Sécurité EMV exposées par Joly (2008 :29) « le serveur assure l'essentiel de la sécurité des transactions des cartes bancaires ».

Il assure :

- le cryptogramme visuel qui correspond aux 3 derniers chiffres inscrits au dos de la carte, à l'emplacement de la signature. C'est le premier dispositif de sécurité important, car il renforce l'identification du client. Les commerçants doivent le demander à leur client lors de tout paiement à distance ;

- La demande d'autorisation : Lors d'une transaction payée à distance avec une carte, la banque du client est contactée par la banque du commerçant : c'est la demande d'autorisation. Cette demande a pour but de vérifier que :
  - le numéro de carte existe ;
  - la date d'expiration est correcte ;
  - la carte n'a pas été signalée comme étant volée ou perdue ;
  - le plafond de paiement de la carte n'a pas été dépassé.

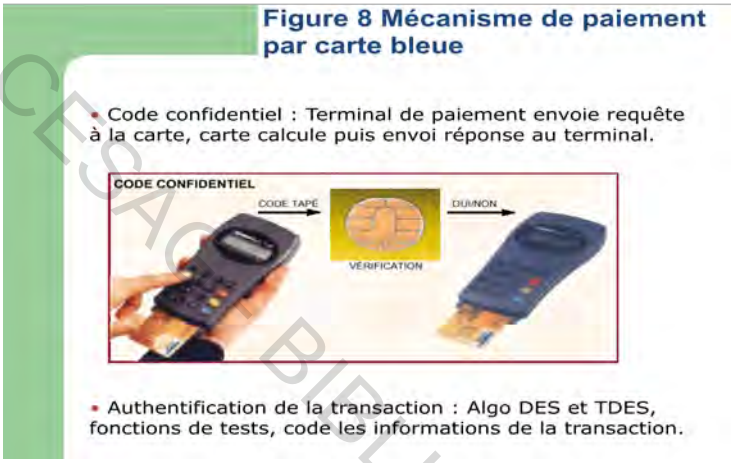
- L'authentification en ligne pour disposer d'une sécurité optimale comme la 3-D Secure, qui leur permet d'acheminer des informations relatives à l'authentification de leurs clients.

Cette architecture permet, à partir de la demande effectuée par le serveur du commerçant, de remonter à la banque de son client, de l'authentifier, de recueillir son accord sur les conditions de réalisation de la transaction (montant, etc.) et d'établir des preuves ou certificat justifiant la transaction effectuée par le client. C'est une chaîne sécurisée qui n'entraîne aucune complexité supplémentaire pour le commerçant car elle est d'ores et déjà intégrée par les fournisseurs de services de paiement.

1.5 Fonctionnement d'une transaction monétique

Nous allons ici faire la distinction entre les deux principales sortes de transactions que sont les retraits au niveau des distributeurs et les paiements au niveau des commerçants. Il y a aussi le mode cash advance qui peut être en quelque sorte associé à un paiement chez un commerçant vu que c'est effectué à l'aide d'un TPE mais aussi peut être associé à un retrait GAB puisqu'il permet de repartir avec de l'argent en liquide et non avec une marchandise.

Figure 4 Mécanisme de paiement par carte bleue



Source : Sécurité EMV (2006)

1.5.1 Les paiements chez les commerçants :

Dans le cadre d'un paiement chez un commerçant, on peut citer trois étapes que sont :

- La transaction en elle-même ;
- la télécollecte ;
- la compensation.

Selon Piedelievre (2007 : 51) « la transaction en tant que telle se déroule en plusieurs étapes distincts et successifs » qu'on peut résumer comme suit :

- le commerçant saisi le montant de la transaction sur le Terminal de Paiement Electronique (TPE) ;
- le client porteur de la carte introduit la carte dans le TPE ;
- le TPE lie et vérifie la validité de la carte. Les contrôles d'acceptation (BIN, nature de la carte…) sont aussi effectués sur le TPE;

- si ces contrôles sont corrects, le client saisi le code PIN. Il dispose de trois tentatives pour saisir le bon code PIN. En cas d'échec aux trois tentatives, la carte peut être bloquée ou confisquée ;
- le système vérifie le code PIN ;
- si la vérification se fait avec succès, l'acquéreur fait une demande d'autorisation au niveau de la banque émettrice. En général, sauf commerçant particulier ou carte à autorisation systématique, un seuil de déclenchement de l'autorisation est fixé. La demande d'autorisation permet à l'accepteur d'avoir l'accord ou le refus de l'émetteur pour effectuer la transaction. Cette demande d'autorisation est gérée par un serveur d'autorisation qui décide si une transaction peut aboutir ou non en fonction des paramètres de la transaction, de la carte et du compte associé. Le serveur d'autorisation est généralement hébergée par la banque propriétaire de la carte mais il peut être délégué à un prestataire externe La demande d'autorisation consiste en partie à comparer le montant de la transaction avec le plafond de la carte et le solde disponible dans le compte. Si le montant de la transaction est supérieur au plafond de la carte ou au solde du compte, la demande d'autorisation n'est pas acceptée. Le porteur doit contacter sa banque pour trouver une solution. La demande d'autorisation permet aussi de vérifier si la carte n'est pas en opposition ou si elle n'est pas expirée. La demande d'autorisation permet enfin d'assurer que la transaction peut bien être effectuée et que la carte existe véritablement. Cela permet d'assurer une garantie pour le commerçant ;
- si la demande d'autorisation est acceptée, un message est affiché sur le TPE, la transaction est sauvegardée, les tickets sont imprimés pour le commerçant et pour le client. Certaines cartes ou terminaux permettent d'effectuer une transaction sans entrer de code PIN. Dans ce cas, la signature du client est requise sur le ticket commerçant. Cependant, si la demande d'autorisation n'est pas acceptée, ou qu'il n'y a pas de connexion réseau pour assurer cette opération, le commerçant peut forcer la transaction. Dans ce cas, si la carte est invalide ou falsifiée, il n'est pas couvert et ne sera pas remboursé ;
- l'opération est terminée, le client repart avec son bien acheté et sa carte.

Par la suite, les opérations sauvegardées au niveau du TPE font l'objet d'une télécollecte pour être envoyées à la banque du commerçant pour traitement. La télécollecte se fait généralement aux heures de faible activité du commerçant.

La compensation entre banques se fait, en fonction de la carte utilisée, à travers des réseaux comme VISA, MASTERCARD, CUP, GIM-UEMOA, qui disposent chacun de leur propre plateforme de compensation. La compensation permet de manière simple de débiter un compte et créditer un autre. Il s'agit ici des deux comptes mis en jeux lors de la transaction. Pour ce faire :

- La banque acquéreur transmet le montant de la transaction, le numéro du porteur et d'autres détails de la transaction à la plateforme de compensation ;
- la plateforme de compensation transmet un message comptable de débit à l'émetteur. C'est à ce moment que l'opération de débit du compte du porteur est transmise au serveur émetteur ;
- la plateforme transmet un message comptable de crédit à l'acquéreur : c'est la transmission de l'opération de crédit du compte accepteur sur le serveur acquéreur.

A la fin de la compensation, le compte du commerçant est crédité et la compte du client est débité.

Une dernière étape consiste au règlement du montant dû entre les banques toujours à travers les réseaux internationaux ou intra communautaires.

1.5.2 Les retraits au niveau des distributeurs

Selon Piedelievre (2007 :60), « pour les retraits au niveau des distributeurs, le principe est à peu près le même que les achats chez les commerçants. La différence principale vient du fait que pour les retraits, la demande d'autorisation et la compensation se font en même temps ». Il n'y a pas ici de phase de télécollecte. Les opérations se font comme suit :

- Le porteur introduit sa carte dans le distributeur ;
- après vérification de la validité de la carte, le porteur entre son code PIN. S'il se trompe trois fois, la carte est capturée par le distributeur ou la carte peut être bloquée ;
- après vérification du code PIN, le client choisi le type d'opération qu'il veut effectuer (consultation de solde, retrait, entre autres) ;
- dans le cas d'un retrait, l'autorisation est obligatoire quelque soit le montant de l'opération ;
- à la fin de l'opération, le porteur retire sa carte et l'argent demandé.

1.6 Les avantages et les risques liés à la monétique

Lors du premier salon monétique régional AHOUANTCHEDE (2012 :12) estimait que « la Réforme des Systèmes de Paiement dans l'UEMOA s'inscrit dans le cadre général de l'assainissement du système financier et de l'accélération du processus d'intégration économique régionale ». La création du Groupement Interbancaire Monétique de l'UEMOA (GIM-UEMOA) va dans ce sens. C'est l'organe chargé de la mise en place de la politique monétique au niveau national et sous régional. Elle possède son propre système de compensation monétique qui est interfacé à STAR-UEMOA pour les règlements.

1.6.1 Avantages de la Monétique

DABO (2006:8) pense que « en Afrique de l'Ouest, le système de paiement par carte bancaire a enregistré des avancées significatives ». C'est aussi l'avis de SEREME Mamadou, adjoint au directeur des systèmes de paiement de la Banque centrale des États de l'Afrique de l'Ouest (BCEAO) qui procédait à l'ouverture d'un séminaire-formation sur « les concepts généraux de la monétique et l'implémentation d'un système monétique », organisé par le Groupe interbancaire monétique de l'Union économique et monétaire Ouest africain (GIM-UEMOA).
Dabo (2005 : 6) reprend les propos de SEREME Mamadou, adjoint au directeur des systèmes de paiement de la Banque centrale des États de l'Afrique de l'Ouest (BCEAO), comme suit : « depuis le lancement du projet de réforme des systèmes de paiement par la BCEAO, pratiquement toutes les banques sont en train de développer des systèmes monétiques dans l'espace UEMOA ». En prenant l'exemple de Dakar, certaines banques de la place qui n'avaient pas de monétique ont maintenant commencé à avoir des systèmes de paiement par carte bancaire. D'après Dabo (2005 : 6), « les banques ont fait des investissements pour acquérir tout d'abord, leur système privatif à l'interne ».

Trois types de services sont proposés par le GIM-UEMOA. Ces services sont exposés dans sa présentation des systèmes de compensations et de règlement (2011 :43) : « ils sont pour au nombre de 3 :

- des services interbancaires permettant d'assurer l'interopérabilité nationale, régionale et internationale des transactions ;

- des services bancaires par délégation qui consistent à des traitements monétiques par délégation permanente pour les établissements non équipés de systèmes monétiques, traitements monétiques par délégation temporaire complémentaire ou en secours de leurs propres systèmes ;
- des services complémentaires c'est-à-dire la centralisation des paiements de factures, des ateliers de personnalisation de cartes, maintenance des parcs GAB, de TPE secours des systèmes informatiques bancaires. »

Toujours selon le GIM (2013 :4) « la monétique interbancaire est opérationnelle depuis le 15 juin 2007. A fin décembre 2012, le réseau GIM comptait 106 membres dont 88 sont connectés à la plateforme interbancaire monétique. »**.** STAR-UEMOA permet aux ordres de virement bancaires d'être réglés en temps réel et imputés sur le compte du bénéficiaire au plus tard à J+2, selon la réglementation en vigueur.

Toujours selon GIM (2013 :6), « le système permet notamment de :

- traiter rapidement et en toute sécurité les paiements de gros montants (susceptibles de créer un risque systémique, lié au fait que la défaillance d'un participant peut entraîner, par effet domino, celles des autres) ;
- réduire les risques de paiement (risque de crédit, risque de liquidité, risque légal, et risque systémique) ;
- faciliter la gestion monétaire et le fonctionnement du marché financier dans l'espace UEMOA ;
- faciliter la gestion de trésorerie des banques de l'UEMOA. »

La BCEAO a pris, une part majoritaire au capital social du groupement, manifestant ainsi sa forte implication dans la promotion du paiement électronique dans l'UEMOA. Le GIM-UEMOA s'est engagé par la même occasion, dans une dynamique du développement du paiement par cartes, à travers l'Acquisition Commerçant.

1.6.2 Les risques de la monétique

Pour des mesures sécuritaires luttant à la cyber-escroquerie, le directeur général de GIM-UEMOA a annoncé un projet concernant la gestion du risque, allant à l'encontre des éventuels

manœuvres des fraudeurs, avec des dispositifs d'alertes efficaces. Les cartes sont dotées d'un micro-possesseur qui permettra de palier aux différentes pratiques des faussaires.
« La fraude des moyens de paiement se diversifie et évolue au même rythme que les paiements sur Internet et voit apparaître une nouvelle forme de cybercriminalité qui augmente de près de 10 % par an et qui devrait se poursuivre jusqu'en 2016 » (Gartner, 2000 : 36).

Les banques ne sont plus maîtresses des règles de sécurité des paiements au détail. L'utilisation des réseaux électroniques ouverts les rend dépendantes de la compétence et de la prudence d'autres opérateurs : des serveurs d'information, des experts de codage, des fournisseurs de logiciels spécialisés, des vendeurs de systèmes de compensation privés, des entreprises de télécommunications.

Ces opérateurs ne sont pas tenus aux mêmes obligations prudentielles que les banques. Il s'ensuit qu'au-delà des risques bien répertoriés des systèmes de paiement, d'autres risques beaucoup plus difficiles à évaluer et à contrôler prennent une grande importance. La vulnérabilité à ces risques est amplifiée par le caractère global, déterritorialisé des réseaux ouverts.

1.6.2.1 Risques de sécurité

L'utilisation par les banques de la monétique et de la monnaie électronique peut être source de conflits entre les différents acteurs des transactions monétaires et financières au Sénégal et pose le problème de sécurisation des systèmes et moyens de paiement au Sénégal. Selon ZONGO (2012 : 11) « les risques de défaillance du réseau d'une banque dus à l'utilisation de la monétique et de la monnaie électronique ne peuvent pas affecter l'ensemble du système de paiement interbancaire au Sénégal ».

Le risque de sécurité, qui fait habituellement partie du risque opérationnel, porte sur des actes intentionnels, notamment la fraude, par lesquels une opération de paiement est enclenchée ou modifiée dans le but de détourner ou de s'approprier frauduleusement des fonds. Ce type de risque peut également comprendre tout acte malveillant ou de sabotage, notamment le piratage informatique ou le déni d'attaques sur le service qui peuvent exposer une partie à une perte financière

1.6.2.2 Risques opérationnels

Vernimen (2007 : 1051) définit le risque opérationnel comme « le risque de pertes directes ou indirectes résultant d'une inadéquation ou d'une défaillance des systèmes internes, des personnes ou provenant d'évènements extérieurs ». On peut donc dire aussi que c'est le risque de perte découlant de l'insuffisance ou de l'échec de processus, de personnes et de systèmes internes, ou d'événements externes. Le risque opérationnel comprend des facteurs tels que les pannes techniques ou l'erreur humaine qui causent ou aggravent les risques de crédit ou de liquidité, ainsi que des événements naturels (ex des cas de force majeure). Le risque opérationnel peut être classé dans les grandes catégories suivantes : fraude interne; fraude externe.

1.6.2.3 Risque de règlement

Vernimen (2007 : 1079) définit le risque de règlement comme « le risque lié au non paiement par l'acheteur des sommes dues au vendeur ». Dans notre cas, il constitue le fait que le règlement dans le cadre de STAR-UEMOA ne se déroule pas de la façon prévue (ex du cas d'un participant n'étant pas en mesure d'honorer à ses obligations nettes). Le risque de règlement comprend à la fois des risques de crédit et de liquidité. Si l'une des parties (participant ou dépositaire centrale banque) n'honore pas à ses obligations de règlements envers une ou plusieurs contreparties, cela peut entraîner un blocage du système à cause du fait que les ordres de transferts et de règlements sont irrévocables.

1.6.2.4 Risque de liquidité

La distinction qui peut être établie entre un risque de crédit et un risque de liquidité est que le risque de crédit se rapporte directement à la possibilité d'une perte, tandis que le risque de liquidité se rapporte à un déficit de trésorerie. Le risque de liquidité se présente soit comme cause immédiate soit comme résultat d'un des autres risques. Par conséquent, dans toute perturbation éventuelle de règlement, le manque de liquidité semble toujours être l'une des conséquences principales de l'incapacité d'un participant d'effectuer un règlement. Servigny (2001 : 30) affirme que « le déficit de liquidité peut être coûteux pour les institutions

financières et aboutir à des emprunts coûteux, des manques aux obligations contractuelles ou la faillite ».

1.6.2.5 Risque systémique

En cas de réalisation du risque de règlement, de crédit ou de liquidité débouchant sur une faillite de l'un des participants, cela peut entraîner le blocage du système de compensation et de règlement susceptible de paralyser l'ensemble du système STAR-UEMOA et SICA UEMOA. Il y a également une possibilité de blocage des règlements en cas de panne du système d'un des grands participants. Un blocage peut se produire lorsqu'un participant n'est pas en mesure de transmettre et de régler des paiements, empêchant ainsi d'autres institutions d'effectuer leurs paiements. En plus, un embouteillage pourrait découler d'un problème opérationnel si un participant immobilise une grande quantité de liquidité (ex lorsque le participant continue de recevoir des paiements d'autres participants mais, pour des raisons techniques, est incapable de libérer les paiements dans le système. Ces différents cas entraînent généralement un risque systémique. Le risque systémique est donc le risque qui touche l'efficacité, la sécurité et le bien-fondé du système de paiement dans son ensemble. De Servigny (2001 : 39) résume parfaitement la définition du risque systémique en disant que c'est « la fragilisation, par le jeu d'un effet domino, de toutes les banques du fait du défaut d'un établissement fortement débiteur ».

1.6.3 La gestion du Risque de la Monétique

Pour ce qui est du risque de règlement, de crédit ou de liquidité pouvant débouché sur un risque systémique la BCEAO demande à tout ses adhérents de constituer des réserves suffisantes en fonction du volume de transaction généralement effectué pour garantir les règlements entre participants. Elle peut se porter garant en dernier ressort en cas de défaillance de deux ou trois participants à la fois (scénario improbable, mais possible).

Par ailleurs, BCEAO (2012 :13) affirme que « des rapports mensuels pour le suivi des transactions et du comportement du système sont élaborés ». Elle a constaté heureusement que jusqu'alors aucun des risques pré cités ne s'est réalisé. Par contre, les responsables du système ont plutôt constaté que le système a effectué des rejets des transactions de certains participants. Ces rejets sont directement imputables aux participants eux même, du fait de la

réalisation d'un risque opérationnel lié à une mauvaise saisie des données dans le système, ou à la vérification de leur statut de participant ou pas. En cas de panne technique, il y a un dispositif de relais et une équipe technique disponible qui peut être aussi déployé chez les participants. Le système vérifie également la disponibilité des fonds avant toute opération. Cela concourt à atténuer ou à limiter le risque de crédit ou de liquidité.

Conclusion Chapitre 1

Ce chapitre nous a appris que SICA-UEMOA est un outil automatisé d'échanges et de règlement des opérations de paiement de masse, entre établissements participants aux niveaux national et sous-régional. Il fait partie des moyens mis en place pour développer la monétique qui devient un élément de plus en plus important pour le développement de notre zone monétaire.

Nous avons aussi à travers ce chapitre avoir une vision globale de la monétique. Les acteurs de la monétique restent multiples et les types de transactions sont très variés.

CHAPITRE 2 : LES NORMES MONETIQUES

Introduction

La monétique, selon Sherif & Al (1999 :3) désigne « l'ensemble des techniques électroniques, informatiques et télématiques permettant d'effectuer des transactions, des transferts de fonds ». Ces transactions représentent sa vulnérabilité d'où la nécessité de sécurisation et de normalisation. La sécurisation de la monétique implique un ensemble de règles juridiques aussi diverses que variées. Celles-ci vont des Traités constitutifs des communautés économiques et monétaires que sont l'UMOA et l'UEMOA aux lois nationales en passant par des normes internationales telles que les normes Lamfalussy et les principes fondamentaux de la Banque des Règlements Internationaux. Comme toute règle juridique, les normes de sécurisation des systèmes de paiement ont besoins, pour leur effectivité et leur efficacité, d`un ensemble d'institutions en charge de leur application effective.

C'est fort de ce constat que nous verrons dans le présent chapitre le cadre juridique de la sécurisation des systèmes de paiements dans l'espace UEMOA avant d'en aborder le cadre institutionnel. Les deux grandes et principales normes dans le monde de la monétique sont la norme Europay Mastercard Visa (EMV) et la norme Payment Card Industry (PCI).

2.1 Le corpus juridique interne à l`UEMOA

Le corpus juridique interne à l'UEMOA s'entend des normes relatives aux systèmes de paiement à leur sécurisation. Ces normes sont d'origine soit législative soit conventionnelle.

2.1.1 Le cadre législatif de la sécurisation des systèmes de paiement

Tout processus d'intégration juridique se caractérise par la coexistence d'au moins deux ordres juridiques. Il s'agit de l'ordre juridique national auquel se superpose celui communautaire d'où la distinction classique entre cadre législatif national et cadre législatif communautaire. Le Directeur de l'exploitation et des normes monétiques du GIM UEMOA a fait une intervention sur ce point lors du salon monétique régional. Ces propos apparus dans le newsteller sont résumées dans les parties ci-dessous : « Deux documents définissent les conditions d'émission de la monnaie électronique par les établissements de l'UEMOA :

- le règlement n° 15/2002/cm/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'union économique et monétaire ouest africaine (UEMOA)
- l'instruction 01/2006/SP du 31 juillet 2006 relatif à l'émission de la monnaie électronique et aux établissements de monnaie électronique.

24 autres documents définissent les normes à respecter par les membres du GIM-UEMOA. Ces documents peuvent être regroupés par groupe en fonction de leur nature :

- contrats Porteur et Accepteur : contrat accepteur et contrat porteur ;
- règles Interbancaires GIM-UEMOA : règles fraude paiement et retrait, règles impayés paiement et retrait, règles générales émission, règles générales commissionnement, règles générales paiement, règles générales retrait, règles opérationnelles de l'émission ;
- normes Interbancaires : normes acceptation TPE, normes autorisations, normes compensations, cycle de vie des cartes GIM-UEMOA, normes émissions, gestion des clés, normes impayés paiements, normes impayés retrait, normes lutte contre la fraude, normes oppositions, normes retrait GAB, normes vente à distance, protocole local interchange specification, protocole switch interface description, protocole point of sale ISO.

Ainsi, peuvent émettre de la monnaie électronique :

- Les établissements bancaires ;
- Les établissements de monnaie électronique (EME) agrés par la BCEAO.

Un opérateur télécoms comme tout établissement peut émettre de la monnaie électronique en coordination avec une banque ou un EME. Dans ce cas, la banque ou l'EME se porte garant de l'ensemble des opérations effectuées par l'opérateur télécoms.
Nous notons ainsi un développement de solutions mobile paiement dans l'espace UEMOA» (ZONGO, 2012 : 11).

2.1.2 Le cadre législatif communautaire

Le droit communautaire des systèmes de paiement au sein de l'UEMOA s'appréhende à travers le diptyque droit communautaire originaire (a) et droit communautaire dérivé (b). Il

faut aussi noter que l'intérêt du droit communautaire est qu'il est là « pour aboutir à une indépendance réelle et un développement commun » (Issa-Sayegh , 1997 : 12).

C'est ainsi que nous avons :

- le droit communautaire originaire relatif aux systèmes de paiement que Issa-Sayegh (1997 :29) qualifie comme ayant « le propre de mettre en place les institutions qui eux mêmes vont sécréter les normes juridiques devant servir de base à l'objectif de sécurisation » ;
- le traité constitutif de l'UEMOA qui met en place un certain nombre d'institutions qui ont une place importante dans la sécurisation des systèmes de paiement que sont : « la Conférence des Chefs d'Etats et de Gouvernements, du Conseil des Ministres, la Commission et la Cour de Justice de l'UEMOA » (SOW, 2002 :104) ;
- les actes additionnels au traité de l'UEMOA qui sont adjoints au traité et ont pour auteur la Conférence des Chefs d'Etat et de Gouvernement ;
- les statuts de la BCEAO qui font partie intégrante du droit communautaire originaire, et cela du fait de leur annexion au corpus articulaire même du Traité de. Ils confient à l'Institution d'émission en son article 26 Section 5 l'organisation et la gestion des chambres de compensation sur les places où elle le juge nécessaire. Le droit primaire ainsi énuméré met donc en place des institutions et des organes en charge d'élaborer les normes juridiques qui ont vocation à régir plus directement les systèmes de paiement. La BCEAO se veut un acteur central pour régulariser tout car comme le dit NTUMBA (1994 : 225) « autant un cadre institutionnel fort, compte tenu de la finalité intégrative ultérieure, peut-il jouer le rôle de locomotive ou de levain, autant un système institutionnel et décisionnel faible ou d'un niveau moyen ne peut-il que difficilement entretenir une dynamique intégrative ascendante ».
- le droit communautaire dérivé relatif aux systèmes de paiement, gage de sécurité dans la mesure où « les normes relevant de cet ordre bénéficient d'un ensemble de principes qui concourent à la garantie de leur effectivité comme les principes de l'applicabilité immédiate et de l'applicabilité directe » (SOW, 2002 :103) ;

2.2 La sécurisation juridique du système monétique

D'emblée, il convient de préciser que le système monétique ne se résume pas au paiement par carte bancaire mais inclut également l'émission de monnaie électronique. « La monnaie électronique est constitutive de la valeur monétaire représentant la créance sur l'émetteur, qui

est : stockée sur un support électronique, émise contre remise de fonds dont la valeur n'est pas inférieure à la valeur monétaire émise et qui est acceptée par des entreprises autres que l'émetteur » (Mostafa, 2007 :48). Le besoin de sécurisation de ce système a conduit à l'élaboration d'un ensemble de mécanismes juridiques destinés à y satisfaire comme l'Instruction No 01/2006/SP du 31 juillet 2006 relative à l'émission de monnaie électronique et aux établissements de monnaie électronique qui définit les conditions prudentielles auxquelles doivent satisfaire les établissements de monnaie électronique pour exercer une telle activité.

2.3 La sécurisation opérationnelle du système monétique

Instruments par excellence de la bancarisation, les cartes bancaires permettent de réduire la circulation de la monnaie fiduciaire et ainsi d'éviter la thésaurisation des ressources financières au sein de l'UEMOA. De plus, elles intègrent les avantages des effets de commerce sans en avoir les inconvénients. « En effet la carte bancaire sert à la fois d'instrument de paiement et de crédit mais n'a pas les coûts exorbitants de la manipulation du papier. Cependant elle n'est pas à l'abri de la fraude qui, dans son cas, emprunte les atours de l'électronique et requiert des barrières technologiques seules à même de freiner son avancée» (COULIBALY, 2010 :1).

La sécurisation des cartes bancaires a nécessité un changement de technologies dans leur conception. Ainsi avec la réforme des systèmes de paiement et la mise en place du système monétique, il a fallu opérer une migration de l'utilisation des cartes à pistes magnétiques vers celles à puces électroniques. Les premières étaient facilement falsifiables car étant conçu avec une technologie rudimentaire qui ne garantissait pas la sécurité des informations contenues dans les pistes magnétiques. La technologie puce apporte de nombreux avantages en matière de paiement notamment la sécurisation des transactions avec une clé cryptographique bien meilleure que celle de la carte à piste magnétique ainsi que l'authentification du porteur de la carte lors d'une transaction. La migration vers la technologie puce s'est appuyée sur la technologie EMV déjà décrite pour une plus grande sécurité des ces instruments.

La sécurisation du système monétique intègre également celle des Terminaux de Paiement Electroniques (TPE) destinés à accueillir les cartes lors des transactions avec les commerçants accepteurs ou lors de retraits sur les Distributeurs Automatiques de Billets ou les Guichets Automatiques de Billets. En effets les fraudes sont non seulement orientées vers les cartes

mais également vers ces terminaux. C'est pour cette raison qu'ils ont également bénéficié de la technologie EMV. En effet, un processus d'homologation des terminaux a été mis en place en 2002 afin de contrôler, par des tests, leur conformité à la norme EMV.

La sécurisation du système monétique est ainsi assurée dans ses dimensions juridiques et opérationnelles même si sécurisation du système monétique doit être attentive aux progrès techniques réalisés dans ce domaine afin d'adapter ses dispositifs pour être réellement efficace.

2.4 La norme EMV

EMV tire son nom des organismes fondateurs Europay, Mastercard et Visa qui sont les trois entreprises ayant coopéré au début pour développer la norme. Selon Dragon (2009 :12) « c'est un standard international pour les cartes à puce mis en place en 1999 pour authentifier les transactions de crédit ou de débit au niveau des terminaux électroniques de paiement ou des distributeurs automatiques de billets. Les trois membres fondateurs (Europay, Mastercard et Visa) ont par la suite été rejoints par JCB en 2004 et par Amex en 2009 ». Cette norme a été créée afin d'assurer l'interopérabilité mondiale des paiements par carte à puce dans un environnement particulièrement sécuritaire.

2.5 Généralités sur l'EMV

Selon DRAGON (2009 :51) « le risque zéro est impossible, et des maillons faibles subsistant dans le système » donc, devant la nécessité d'améliorer la sécurité du paiement et des retraits par cartes, les principaux acteurs de la monétique dans le monde ont décidé de passer à la technologie carte à puce. L'évolution vers une carte à puce fait partie de l'évolution logique de la carte bancaire, comme de tout moyen de paiement.

La norme EMV définie et spécifie l'interaction entre les cartes à puces et les outils d'acceptations tels que les GAB et les TPE. « Elle décrit le déroulement d'une transaction et l'échange d'informations nécessaires à son fonctionnement sécuritaire. Ses principales caractéristiques sont :

- l'interopérabilité internationale ;
- la vérification et le chiffrement de la clé personnelle par la puce ;

- la gestion plus ouverte de plusieurs applications sur la carte » (TAVERNIER, 2006 :43).

Ses évolutions sont gérées par EMVCo. C'est un organisme exploité par Visa International, MasterCard International et JCB International.

2.5.1 Spécifications EMV et caractéristiques mécaniques de la carte

Selon TAVERNIER (2006 :83) « les Spécifications EMV sont basées sur la norme ISO/IEC 7816 et doivent être lues conjointement avec la norme ISO ». Ces spécifications doivent être utilisées par fabricants de terminaux, les concepteurs de systèmes de paiement et les institutions financières qui implantent des applications financières pour garantir une interopérabilité. Il y a aussi d'autres caractéristiques mécaniques comme la fait que la carte doit être opaque aux rayons UV et résister aux détériorations de sa surface.

2.5.2 Notion de donnée de carte

Les données cartes correspondent aux données liées au porteur de la carte qui sont fournies ou récupérées lors d'une transaction. Selon GUEULLE (2004 :57) « ces données peuvent être classées de deux sortes : les données de porteurs de carte qui doivent faire l'objet de protection et les données d'authentification sensibles dont le stockage est interdit après l'autorisation de la transaction ».

Les données devant faire l'objet de protection sont le numéro de compte primaire, le nom du titulaire de la carte, le code service et la date d'expiration. Les données sensibles interdites de stockage sont quant à elles composées des données de bandes magnétiques ou leur équivalents stocké sur la puce, le cryptogramme visuel à trois chiffre au dos de la carte utilisé pour les transactions à distance et la version chiffrée du code PIN.

Toutes ces données sont considérées comme sensibles car elles peuvent permettre d'effectuer des transactions de paiement frauduleuses, elles peuvent permettre d'identifier le porteur, elles peuvent permettre de récolter des informations sur les cartes de paiement.

2.5.3 Les objectifs de la norme EMV

Cette norme « vise principalement : une augmentation de la sécurité et de la rapidité des transactions ; une baisse des coûts de transaction pour les commerçants ; une authentification des transactions et une diminution de la fraude ». (GUEULLE, 2004 :59).

La norme EMV vient dans un contexte multi-applicatif. Ceci permet à la carte bancaire de supporter plusieurs applications en sus de celles de paiement et de retrait actuellement utilisées. Les cartes à puce EMV ont été conçues et introduites pour réduire la fraude. Il a été clairement démontré que dans les pays où a été déployé le système EMV, il existe une baisse mesurable et significative de la fraude lors des transactions.

La norme permet aux banques de renforcer la sécurité lors de l'utilisation de la carte. Par ailleurs, l'offre multi-applicative qu'elles peuvent, développer grâce à la puce leur donne l'opportunité d'intégrer des services non bancaires dans leurs produits monétiques. La puce permettant ainsi d'intégrer des systèmes d'exploitation dans les cartes. Elle permet aux acquéreurs (banques, commerçants et DAB) et aux banques émettrices de cartes de mieux gérer leurs risques. La revue de littérature montre donc que l'apport sécuritaire majeur de l'EMV est le renforcement de la protection contre la fraude sous plusieurs aspects.

2.5.4 Avantages de la norme EMV

Chaque acteur trouve des avantages à tirer de la norme EMV. Les avantages de l'EMV pour chaque acteur sont les suivants :

- pour la banque nous avons l'amélioration de l'image et de la notoriété ; la conquête et la fidélisation de la clientèle à travers une meilleure sécurisation et de nouveaux services à valeur ajoutée pour le client; le bénéfice de nouvelles opportunités marketing liées à la montée en gamme et à la stratégie de remplacement des cartes ; l'augmentation du nombre de transactions ; l'amélioration de la rentabilité via l'augmentation des volumes de transactions et la diminution des frais liés à la fraude,
- du côté du porteur, on peut citer les avantages suivants la valorisation de l'utilisation de sa carte et la montée en gamme proposée ; les nouveaux services liés à la fois aux aspects sécuritaires et aux offres qui pourront être développées dans le cadre du multi-applicatif,

- pour les commerçants et les partenaires les avantages qui peuvent être notés sont la conquête et fidélisation de la clientèle et la meilleure personnalisation des campagnes de communication.

Un autre avantage technique et sécuritaire est comme l'a dit Urien (2008 : 86) « dans la norme EMV les informations élémentaires (ou data element) sont organisées sous forme de Data Objects (ou DO) décrits par la norme ISO 7816 ».

2.5.5 Le transfert de responsabilité

A la suite de la mise en place de la norme EMV, le système de transfert de responsabilité a été instauré. Les commerçants qui n'ont pas des terminaux qui répondent aux normes EMV endossent la responsabilité des transactions frauduleuses commises dans leur établissement. Mais pour cela il faut d'abord que la carte utilisée soit une carte à puce pour que ce transfert se fasse.

Le transfert de responsabilité plus connu sous le nom de « liability shift » rend la migration à la norme EMV impérative. En effet, en cas de fraude ou d'impayé lors d'une transaction effectuée par une carte EMV, le transfert de responsabilité fera porter la responsabilité de la fraude sur l'entité qui ne sera pas équipé en matériel EMV. Ceci implique qu'émetteurs et acquéreurs se dotent des moyens adéquats (émission de cartes à puce, distributeurs de billets et terminaux de paiement certifiés EMV).

La migration vers les normes EMV ne s'est pas faite en même temps sur toutes les parties du monde. Le nouveau standard à été adopté progressivement, d'abord par les pays européens, puis un peu partout dans le monde. Les États-Unis sont le dernier pays en Amérique du Nord et l'un des derniers pays du monde à ne pas avoir encore commencé l'implantation du standard EMV.

2.5.6 Les limites de la norme EMV

Depuis que la technologie de la puce a été développée et adoptée, elle a permis de conserver des taux de fraude relativement faibles, mais elle a également prouvé qu'elle n'était pas sans faille.

« L'absence ou la faiblesse des vérifications des transactions en ligne et la conservation de la bande magnétique sur les cartes de paiement favorisent la fraude sans la présence physique de la carte » (TAVERNIER , 2006 :142). C'est par exemple le cas pour les transactions à distance faites par Internet, par téléphone, etc. ces transactions peuvent être faites sans la présence physique de la carte.

L'autre limite de la norme se situe au niveau des transactions fall back qui est une technique qui permet de lire la piste lorsque la lecture de la puce est impossible.

Une carte seule, volée sans code confidentiel peut être utilisée dans le terminal d'un commerçant qui autorise les transactions par la bande magnétique. Les transactions fall back concernent aussi les DAB.

2.6 La norme PCI

Le terme « PCI » (Payment Card Industry) désigne généralement le Conseil des normes de sécurité du secteur des cartes de paiement (PCI SSC ou « Conseil du SCP »). Le Conseil du SCP est un forum international ouvert qui a été lancé en 2006 par MasterCard Worldwide et quatre autres marques de paiement afin de créer et de gérer des normes de sécurité visant à protéger les données sur les cartes de paiement. La norme prépondérante est la norme de sécurité des données PCI DSS (PCI Data Security Standard). Lorsqu'on demande à un commerçant son statut de conformité à la sécurité des données, on veut généralement savoir s'il respecte les processus et les contrôles de sécurité de la PCI DSS. « Le principal objectif de la PCI DSS est de réduire le risque de perte de données sur les cartes de paiement en prévenant, en détectant et en contrant les infractions ou les attaques potentielles qui pourraient mener à la compromission des données sur les comptes » (ROEBURCK, 2009 :10). En d'autres termes, la PCI DSS sert à protéger les données sur les cartes de paiement contre les menaces criminelles et à réduire le risque d'atteinte à la sécurité des données pour les commerces de toutes tailles.

ROEBURCK (2009 :15) explique que : « les Normes PCI décrivent en détail les exigences en matière de sécurité pour les commerçants et prestataires de services stockant, traitant ou transmettant des données de titulaire de carte ». Pour attester de la conformité aux Normes PCI DSS (Data Security Standard) les commerçants et prestataires de services peuvent être tenus de se soumettre à des Balayages de sécurité PCI périodiques, réalisés conformément aux

exigences de chaque société de carte de paiement. Ils constituent un outil indispensable, destiné à être utilisé en liaison avec un programme de gestion des vulnérabilités.

2.6.1 Les différentes composantes de la norme PCI

« Les normes PCI (Payment Card Industry) sont divisées en trois parties qui sont : les PCI – PED, les PCI – PA, les PCI – DSS » (ROEBURCK, 2009 :9). Nous nous concentrerons plus spécifiquement sur les PCI-DSS tout au long de ce mémoire.

Les PCI - PED (PIN Entry Device) sont obligatoires pour les nouveaux TPE. Cette norme consiste à sécuriser le clavier PIN PAD en protégeant la saisie du code confidentiel, et à bloquer le terminal en cas d'intrusion frauduleuse ou accidentelle. Ce référentiel concerne uniquement les constructeurs de dispositifs de saisie de code.
Les PCI – DSS (Data Security Standards) instaurent des règles sécuritaires strictes sur le transport et la conservation des données sensibles (par exemple le numéro de carte) et interdit le stockage des éléments secrets (par exemple code confidentiel, cryptogrammes de validation de la carte). Il s'applique aux systèmes d'information des différents acteurs de la chaine de paiement.
Les PCI – PA (Payment Application) définissent les critères de sécurisation des données sensibles au niveau de l'application de paiement sur les systèmes d'acceptation. Ce référentiel s'applique aux sociétés ou prestataires qui développent des applications de paiement quand celles-ci sont vendues. Ce référentiel vise à minimiser les failles des applications de paiement.

Certains auteurs trouvent que le PCI-PA et PCI PED ne sont pas suffisants. Ceci s'explique par le fait que si les logiciels et équipements sont vendus comme conformes aux normes, cela n'implique pas une conformité automatique pour celui qui utilise ces éléments. Nous allons cependant axer la suite du chapitre sur la norme PCI DSS qui est un référentiel de sécurisation des données carte bancaires s'appuyant sur les bonnes pratiques. Ce référentiel s'applique à toute entité qui traite et ou stocke des données de carte.

En réalité, « la norme PCI-DSS liste un ensemble de points de contrôles relatifs aux systèmes d'informations qui capturent, transportent, stockent et traitent des données de cartes bancaires. Les points de contrôles sont relatifs à des techniques informatiques mais également à des procédures et à des contrôles organisationnels sur ces systèmes » (LEKINGANI , 2011 : 31).

2.6.2 Le PCI SSC

C'est en 2006 qu'est né un organisme indépendant appelé PCI SSC (Payment Card Industry Security Standards Council) pour prendre en charge le développement, la gestion, l'application des normes PCI. Le PCI SSC fourni dans son site internet plusieurs documents sur la norme PCI et sur sn application. Parmi cette documentation, le document nommé « condition et procédures d'évaluation de sécurité » est celui qui a le plus attiré notre attention. L'étude et la synthèse de toute cette documentation a permis de rédiger cette partie sur les normes PCI.

2.6.3 Les exigences de la norme PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) est un ensemble homogène de normes de sécurité pour la gestion des données de carte valables dans le monde entier. Les directives qui y sont définies s'appliquent à toutes les parties – commerçants, Acquirers, Service Providers etc. – qui transmettent, traitent et/ou stockent des données de carte**.**

Confrontées à la constante augmentation de l'utilisation abusive des données de carte, les principales organisations de cartes – Visa, MasterCard, JCB, Diners Club et Discover – ont développé les normes PCI DSS afin de renforcer la sécurité des paiements par carte et d'améliorer la protection des commerçants et des titulaires de carte. En principe, selon CALDER, (2014:41) « toute partie impliquée dans le traitement de transactions par carte est tenue de respecter les normes de sécurité ». Il s'agit donc des commerçants, des Payment Service Providers, des Data Storage Entities, des acquéreurs, etc.

Les entreprises concernées doivent faire vérifier régulièrement l'ensemble de leurs mesures en matière de sécurité et fournir la preuve qu'elles ont effectivement pris toutes les mesures techniques et structurelles nécessaires en termes de sécurité. Cela va du questionnaire d'auto-évaluation au contrôle sur site des dispositifs de sécurité.

Les avantages de PCI DSS se présentent comme suit :

- Identification et réduction des risques ;
- Prévention de la perte de réputation ;

- Réduction des risques de conséquences pécuniaires en cas de vol de données de carte ;
- Protection accrue de l'ensemble des données clients ;
- Renforcement de la confiance des clients grâce à la sécurité accrue.

Tous les acteurs qui entrent en jeux dans le circuit du paiement par carte bancaire doivent appliquer certaines conditions pour être conformes aux exigences.
La norme PCI DSS contient 12 conditions opérationnelles et techniques essentielles, définies par le Conseil des normes de sécurité PCI (PCI SSC).

WILLIAMS (2013 :27) nous énumère ces conditions comme suit : « Le PCI DSS fixe 12 exigences fermes qui doivent impérativement être respectées.

A - Mise en place et maintenance d'un réseau sécurisé
- Exigence 1: Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de cartes ;
- Exigence 2: Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.

B - Protection des données de titulaire de carte
- Exigence 3: Protéger les données de titulaire de carte stockées ;
- Exigence 4: Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts.

C - Maintenance d'un programme de gestion des vulnérabilités
- Exigence 5: Utiliser des logiciels antivirus et les mettre à jour régulièrement ;
- Exigence 6: Développer et gérer des systèmes et des applications sécurisés.

D - Mise en œuvre de mesures de contrôle d'accès strictes
- Exigence 7: Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître ;
- Exigence 8: Attribuer un ID unique à chaque utilisateur d'ordinateur ;
- Exigence 9: Restreindre l'accès physique aux données de titulaire de carte.

E - Surveillance et test réguliers des réseaux
- Exigence 10: Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte ;
- Exigence 11: Tester régulièrement les processus et les systèmes de sécurité.

F - Gestion d'une politique de sécurité des informations

- Exigence 12: Respecter les lignes directrices concernant la sécurité de l'information pour les employés et sous-traitants. »

2.6.4 Les objectifs de la norme PCI DSS

Plutôt que de se concentrer sur une catégorie de fraude spécifique, la norme PCI DSS cherche à protéger les données d'identification sensibles et celles du titulaire, partout où ces données sont présentes dans l'écosystème de paiement, limitant ainsi la disponibilité de ces données pour les fraudeurs.

« La norme PCI DSS atteint ses objectifs de sécurité de deux manières : d'abord en garantissant l'intégrité des composantes du système qui conduisent aux données d'identification sensibles et à celles du titulaire de carte, contre des attaques physiques et logiques puis en protégeant la confidentialité des données du titulaire lorsqu'elles sont stockées au sein d'un environnement donné, ou celle des données du titulaire et d'identification sensibles lorsqu'elles sont transmises sur un réseau ouvert ou public » (REFALO , 2012 :104).

La norme PCI DSS a été développée dans le but de renforcer la sécurité des données des titulaires de cartes et de faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. Elle sert de référence aux conditions techniques et opérationnelles conçues pour protéger les données des titulaires de cartes. Elle s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, acquéreurs, émetteurs et prestataires de service, ainsi que toutes les autres entités qui stockent, traitent ou transmettent des données de titulaires de cartes. Elle consiste en un ensemble de conditions minimum pour la protection des données de titulaires de cartes et peut être renforcée de contrôles et pratiques supplémentaires pour réduire encore davantage les risques.

2.7 Autres normes et lois de la monétique

2.7.1 La norme ISO 27001

Selon Carpentier (2009 : 21), la norme ISO 27001 est « la norme principale des besoins en système de gestion de la sécurité de l'information, plus connue sous la forme BS 7799-2. ». C'est une norme qui a des similitudes avec les PCI DSS mais elle n'est, contrairement à cette dernière, pas le résultat d'une analyse effectuée par les organismes cartes. Elle est donc assez souple quant au périmètre, aux mesures de sécurité, à la conformité et à la mise en place. Elle a été construite de façon à s'adapter à des entreprises d'activité très différentes et à des risques variés. Son but premier est d'organiser la sécurité en général.

C'est une norme qui suggère des mesures de sécurité mais ne les rend pas obligatoire. Ceci laisse la possibilité à chaque organisation de décider des mesures à mettre en place en fonction de la sensibilité aux risques.

2.7.2 Autres normes ISO traitant du système monétique

ZONGO (2012 : 11) regroupe les normes ISO intéressant le système monétique de l'UEMOA en 3 parties que sont : « les normes relatives à la sécurité, les normes relatives à la qualité et les normes relatives à la protection des données ».

- Les normes relatives à la sécurité : parmi les normes relatives à la sécurité, nous pouvons citer la norme « ISO/IEC TR 13335 Technologies de l'information » qui donne les lignes directrices pour la gestion de la sécurité des technologies de l'information ; la norme « ISO TR 13569 Banque et services financiers liés aux opérations bancaires » qui porte sur la sécurité de l'information .

- Les normes relatives à la qualité : nous citerons pour ce cas la norme « ISO 9000 » qui touche au management de la qualité et l'assurance de la qualité.

- Les normes relatives à la protection des données : la principale norme dans ce domaine est la norme « ISO 9364 » sur les messages bancaires télétransmis.

Cela s'est traduit par un certain nombre de normes internationales dont le tableau ci-dessous donne une liste aussi complète que possible dans le cas des cartes en général.

Tableau 1 Normes ISO concernant les cartes monétiques

Norme ISO	Titre officiel
ISO 7810	Identification Cards – Physical Characteristics .Cartes d'identification – Caractéristiques physiques
ISO 7811-1	Identification Cards – Recording Technique Embossing Cartes d'identification – Techniques d'embossage
ISO 7811-2	Identification Cards – Recording Technique Magnetic Stripe Cartes d'identification – Techniques d'enregistrement magnétique
ISO 7811-3	Identification Cards – Recording Technique Location of Embossed Characters on ID 1 Cards Cartes d'identification – Emplacement des caractères embossés sur les cartes de type ID 1
ISO 7811-4	Identification Cards – Recording Technique Location of Read-Only Magnetic Tracks – Tracks 1 and 2 Cartes d'identification – Position des pistes magnétiques à lecture seule – Pistes 1 et 2
ISO 7811-5	Identification Cards – Recording Technique Location of Read-Xrite Magnetic Tracks – Track 3 Cartes d'identification – Position des pistes magnétiques à lecture/écriture – Piste 3
ISO 7812-1	Identification Cards – Identification of Issuers Part 1 : Numbering System Cartes d'identification – Identification de l'émetteur, partie 1 : système de numérotation
ISO 7813	Identification Cards – Financial Transaction Cards Cartes d'identification – Cartes pour transactions financières
ISO 7186-1	Identification Cards – Integrated Circuits Cards with Contacts – Physical Characteristics Cartes d'identification – Cartes à circuits intégrés avec contacts – Caractéristiques physiques
ISO 7816-2	Identification Cards – Integrated Circuits Cards with Contacts – Dimension and Location of the Contacts Cartes d'identification – Cartes à circuits intégrés avec contacts – Dimension et position des contacts
ISO 7816-3	Identification Cards – Integrated Circuits Cards with Contacts – Electronic Signals and Transmission Protocols Cartes d'identification – Cartes à circuits intégrés avec contacts – Signaux électroniques et protocoles de transmission
ISO 7816-3 Amendment 1	Protocol type T = 1, Asynchronous Half Duplex Block Transmission Protocol Protocole T = 1, protocoles asynchrone semi-duplex à transmission par blocs
ISO 7816-3 Amendment 2	Revision of Protocol Type Selection Révision du mode de sélection de protocole
ISO 7816-4	Identification Cards – Integrated Circuits Cards with Contacts – Interindustry Commands for Interchange Cartes d'identification – Cartes à circuits intégrés avec contacts – Commandes inter-industries

ISO 7816-5	Identification Cards – Integrated Circuits Cards with Contacts – Number System and Registration Procedure for Application Identifier Cartes d'identification – Cartes à circuits intégrés avec contacts – Système de numération et procédure d'enregistrement pour l'identification des applications
ISO 1177	Information Processing – Character Structure fort Start/Stop and Synchronous Character Oriented Transmission Traitement de l'information – Structure des caractères pour les échanges synchrones orientés caractères

Source : Organisation Internationale de la Normalisation (2005)

En ce qui concerne la carte à puce, trois normes principales sont à extraire de ce tableau :

- La norme ISO 7816 – 1 précisant les caractéristiques physiques de la carte ;
- la norme ISO 7816 – 2 définissant la position et le brochage des contacts de la carte à puce ;
- la norme ISO 7816 – 3 définissant les niveaux électriques et les chronogrammes de bas niveau qui régissent le dialogue avec les cartes à puce ;
- la norme ISO 7816 – 4 enfin, définissant les différentes commandes de base des cartes à puce.

2.7.3 Quelques lois en vigueur au Sénégal :

Parmi les lois et règlements en vigueur au Sénégal, nous pouvons citer la loi N° 2008-12 sur la protection des données à caractère personnel vise principalement la protection de la vie privée et la loi sur les transactions électroniques qui, à travers les règles qu'elle édicte, veut parvenir à favoriser le développement du commerce électronique.

Conclusion chapitre 2

En résumé, ce chapitre nous a permis de voir que la mise en œuvre de mécanismes d'authentification rend difficile voire impossible la copie des informations contenues dans la carte ainsi que la duplication de la carte elle-même. Ils facilitent des services sûrs et rapides liés à l'utilisation de la puce qui offre une sécurité permettant d'effectuer des transactions off line, améliorant le service apporté au porteur de carte et réduisant ainsi les frais téléphoniques des banques et des commerçants. En outre, ces normes EMV permettent d'avoir des services diversifiés offerts par la possibilité de gérer plusieurs applications sur la puce (programme de fidélité, porte-monnaie électronique, assurance...).

En plus de la norme EMV, nous avons la norme PCI, les normes ISO et certains lois et règlements qui permettent de réguler le fonctionnement de la monétique. Les lois et règlements doivent être étoffés.

CHAPITRE 3 : METHODOLOGIE DE RECHERCHE

Introduction

Dans ce chapitre, nous vous présenterons la démarche suivie, le modèle de recherche utilisé pour mener à bien ce mémoire. Cette recherche a été faite avec l'aide d'outils de collecte de données nous permettant de recueillir les informations dont nous avons besoin. Nous présenterons ensuite dans ce chapitre des outils de collecte et d'analyse.

3.1 Le modèle d'analyse

La réalisation de ce mémoire se basera principalement sur le modèle d'analyse résumé dans le tableau ci-dessous. A la suite du tableau, nous vous présenterons de manière plus détaillée les différentes étapes de l'analyse afin de mieux faire comprendre les objectifs attendus.

Pour élaborer le modèle d'analyse, nous avons utilisé l'approche normative car la monétique est soumise à des normes qui font office de règles. Parmi ces normes, celles que nous allons prendre en compte ici sont les normes PCI et EMV.
Cette approche va permettre de voir si les règles sont respectées et aussi de mettre en exergue les axes à améliorer.
Ceci nous à permis d'élaborer le tableau ci-après :

Tableau 2 : Présentation du modèle d'analyse

Phases	Etapes	Outils
Préparation	Prise de connaissance du CSMM, de la monétique et de la situation actuelle	Analyse documentaire Observation Entretien
	Prise de connaissances des normes PCI et des normes EMV	Analyse documentaire Entretien
	Préparation des outils d'analyse et de collecte de données	Analyse documentaire

Réalisation	Description et analyse de la situation actuelle	Analyse documentaire Observation
	Comparaison de ce qui se fait par rapport aux normes PCI et EMV	Analyse documentaire Observation Entretien
Finalisation	Analyse des résultats	Analyse documentaire
	Recommandations	Analyse documentaire

Source : Nous mêmes inspiré de la revue de littérature

- Prise de connaissance du CSMM, de la monétique et de la situation actuelle :

Cette étape nous permettra d'abord de voire comment fonctionne le CSMM, comment l'activité des filiales est gérée par le CSMM. Puisque toute l'activité du CSMM tourne autour de la monétique, cette compréhension permettra de savoir d'une manière générale ce qu'est la monétique, quels sont les principes de base de la monétique. Cette partie permettra surtout d'avoir une idée de l'existant tout en nous familiarisant à la monétique et au fonctionnement d'un centre des services mutualisés.

- Prise de connaissance de normes EMV et des normes PCI

C'est au cours de cette étape que nous prendrons connaissance et ferons une étude des principales normes qui régissent le monde de la monétique et auxquelles le CSMM et les filiales qu'elle gère doivent se conformer.

- Préparation des outils de collecte et d'analyse de données

Cette étape nous permettra de préparer, rassembler, recenser toutes les méthodes et outils pouvant nous permettre de recueillir les informations qui nous seront utiles pour la rédaction de notre mémoire.

- Description et analyse de la situation actuelle

C'est lors de cette étape que nous feront une description du fonctionnement du CSMM, du travail qui y est mené et de la relation entre le CSMM et ses filiales.

- Comparaison de ce qui se fait par rapport aux normes EMV et PCI

Dans cette partie, nous utiliserons les normes cités plus haut comme référentiels pour les comparer aux pratiques du CSMM et de ces filiales.

- Analyse des résultats

Nous allons lors de cette étape étudier et examiner les résultats de la comparaison effectuée lors de l'étape précédente afin de voir à quel point les normes sont appliquées.

- Recommandations

Cette partie consistera à fournir des recommandations par rapport aux conclusions de notre analyse afin de pouvoir fournir des recommandations pouvant permettre l'amélioration du fonctionnement du CSMM toujours dans le respect des normes.

3.2 Les outils de collecte des données

Le choix de la méthode dépend de la stratégie de collecte des données, du type de variable, de la précision souhaitée, du point de collecte et des compétences de l'agent recenseur. Les relations qui existent entre une variable, sa provenance, et les méthodes concrètement utilisées pour sa collecte peuvent aider à choisir la méthode appropriée. Les principales méthodes de collecte sont les suivantes:

- les questionnaires: ce sont des formulaires qui sont remplis et retournés par les déclarants. C'est une méthode peu coûteuse ;
- les entretiens: ce sont des formulaires qui sont remplis à l'occasion d'un entretien avec le déclarant. Plus coûteux que les questionnaires, ils sont préférables pour des questions plus complexes ;
- les observations directes: les mesures effectuées directement sont la méthode la plus précise pour de nombreuses variables, comme les captures, mais sont souvent coûteuses.
- les déclarations: la principale alternative aux mesures directes consiste à demander aux banquiers et autres intéressés de rendre compte de leurs activités. Le système des déclarations peut être renforcé par une obligation légale et par des mesures directes.

Vu le contexte dans lequel s'est déroulé la préparation et la rédaction du mémoire, les trois outils de collecte de données choisis sont le guide d'entretien, l'observation, l'analyse documentaire. Ces trois outils de collecte de données ont été choisis car nous avons jugés qu'ils sont les plus capables de nous donner l'information que nous recherchons tant qualitativement que quantitativement.

Les premières données collectées concernent la littérature existante sur la monétique et la monnaie électronique dans le monde en générale, dans l'UEMOA et au Sénégal en particulier. Il faut toutefois préciser que dans les deux derniers cas, il n'était pas facile de rentrer en

possession de l'information du fait, de la quasi-absence, sinon de l'insuffisance de documentation sur le sujet. Cependant, plusieurs centres de documentation ont été sollicités, il s'agit de la bibliothèque de l'Agence Nationale de Statistique et de la Démographie (ANSD), de la bibliothèque de la BCEAO, de l'Université Cheikh Anta Diop et du Groupe Interbancaire Monétique de l'UEMOA (GIM-UEMOA). Nous avons également consulté quelques sites internet comme le site de la BCEAO, du GIM-UEMOA et de l'ANSD

3.2.1 Le guide d'entretien

Selon Nicolas Lefèvre dans Méthodes et techniques d'enquête, (2001 :42) : « l'entretien revêt des processus fondamentaux de communication et d'interaction humaine. L'entretien engage deux personnes en vis-à-vis et à ce titre ne peut être considéré comme un simple questionnaire où on est dans une relation anonyme. Des rapports sociaux se jouent dans un entretien ».
Nous avons décidé de nous entretenir avec le Directeur du Centre, deux chefs de projet et un agent d'exploitation pour avoir un point de vue selon les différentes positions. Ça a permis de prendre en charge les intérêts et points de vue des différentes parties.
Nous avons organisé des entretiens de 15 à 30 minutes en essayant d'avoir l'avis des différents interlocuteurs sur les points suivant :

- l'organigramme et l'organisation du CSMM,
- une description du travail effectué,
- les ambitions personnelles,
- les attentes,
- la vision du future pour le CSMM

Nous avons décidé d'utiliser la méthode de l'entretien semi-directif car nous disposions d'un certain nombre de thèmes ou de questions guides, relativement ouvertes, sur lesquels l'interviewé devait réponde. Mais nous ne posions pas forcément toutes les questions dans l'ordre dans lequel nous les avions notés et sous leur formulation exacte. Nous avions avant tout affaire à des collègues et nous connaissions l'environnement, donc nous avons essayé de rendre l'entretien aussi convivial et informel que possible.
Nous avons cherché une discussion avant tout, à échanger des points de vue s'appuyez sur des faits objectifs tirés de notre travail de tous les jours vu que c'est notre environnement de travail.

Nous avons en annexe 2 le guide d'entretien utilisé dans ce mémoire. Ce guide nous a permis de préparer l'entretien avec le Directeur du CSMM et nous a servi de repère tout au long de l'entretien.

Le choix s'est porté d'abord sur le Directeur car c'est le personnage central du CSMM qui a été là depuis le début du projet. Nous avons donc jugé qu'il est bien placé pour nous donner les informations dont nous avons besoin. Nous avons aussi interrogé les responsable du pôle projet et le correspondant informatique du CSMM pour en savoir plus sur le niveau d'application de la norme PCI DSS.

3.2.2 L'observation

L'observation est définie par MOUCHTOURIS (2012 : 17) comme « considérer attentivement une chose en vue de mieux connaitre ». Connaissant notre but, le but de notre recherche, nous mobiliserons donc notre attention en vue d'obtenir les informations souhaitées.

« La fiabilité des données collectées par l'observation repose sur la constance de l'observation et la réplication des résultats » (Gagnon, 2005 : 21). Etant donné que nous étions nous même employé du CSMM que nous fréquentions tous les jours nous avons pu observer son fonctionnement de façon constante, permanente pendant plusieurs mois. Cette observation a aussi permis de valider les données recueillies lors de l'entretien en confrontent les informations recueillies.

Nous avons observé le travail au quotidien, la manière dont les normes et procédures sont appliquées, le fonctionnement d'une manière pratique du CSMM. Tout ceci doit se faire de manière impartiale. Cette observation nous a permis de pouvoir faire une comparaison entre les informations recueillies lors de l'observation et les informations recueillies lors de l'analyse documentaire.

3.2.3 L'analyse documentaire

Selon Pomart (2001 :72) , « l'analyse documentaire est l'opération essentielle déterminant la qualité ou la non-qualité d'une recherche d'information qui en est l'aboutissement : elle consiste à extraire d'un texte tout son sens, pour le transmettre à qui en a besoin ».

En choisissant l'analyse documentaire, nous nous sommes attelé à faire l'analyse du contenu des documents qui sont à notre portée. Ce sont des documents sur la monétique, ou sur la mutualisation des services. Ces documents sont d'origines et de formes diverses. Nous avons ainsi pu consulter aussi bien les ouvrages des auteurs que des documents internes de l'entité sur laquelle le travail porte. Ces documents internes sont entre autres les procédures, les mémos, les comptes rendus, les processus.

Nous avons aussi beaucoup consulté des sites internet et consulté des livres en ligne sur la monétique et les normes car dans les bibliothèques du CESAG et de DAKAR en général, les documents sur la monétique font défaut.

Conclusion Chapitre 3

Les choix que nous avons opérés nous permettront sans nul doute de collecter, analyser et proposer des recommandations à la Direction Générale de CSMM. Les difficultés rencontrées se situent au niveau de notre méconnaissance du terrain comblée par la disponibilité des acteurs de la structure d'accueil.

CONCLUSION DE LA PREMIERE PARTIE

Les causes de la faible bancarisation sont multiples. Il y a des facteurs structurels tels que le niveau de développement économique, social, institutionnel et juridique qui déterminent l'environnement global et des facteurs particuliers au secteur bancaire comme les conditions d'ouverture des comptes, le taux des crédits à la clientèle, la taille des banques, etc.

Tout au long de cette partie, nous nous sommes surtout attelé à présenter de manière théorique le concept essentiel évoqué dans notre thème à savoir la monétique. Face aux multiples risques et menaces auxquels les activités liées à la monétique font face, les professionnels du milieu et certains organismes ont mis en place des normes pour assurer la fiabilité et la sécurité des transactions monétiques.
Les réformes élaborées par la BCEAO seront sans nul doute ce qui permettra à terme de toucher le maximum de population de la zone pour une utilisation optimum de la carte bancaire.

DEUXIEME PARTIE : CADRE PRATIQUE

INTRODUCTION DE LA DEUXIEME PARTIE

Le but principal de cette partie est, après une présentation de la monétique et de ces normes dans la partie précédente, de décrire et d'analyser la situation réelle du CSMM. Ceci permettra de mieux comprendre le fonctionnement du CSMM mais surtout de comparer ce qui se fait actuellement (en son sein et au sein des filiales qu'il gère) par rapport aux normes monétiques.

La deuxième partie comprendra un chapitre 4 qui fera une présentation du CSMM (historique, missions, objectifs) ; un chapitre 5 sur les activités du CSMM et l'application des normes ; enfin, nous aurons un chapitre 6 qui fera une analyse des activités et des recommandations.

CHAPITRE 4 PRESENTATION DE CSMM

Introduction

Pour 2011, le Gouvernement du Sénégal a prévu une amélioration de la croissance, dans un contexte de maîtrise des fondamentaux de l'économie. De fait, ses perspectives de développement économique et financier à moyen et long terme s'appuieront sur le Document de Politique Economique et Sociale (2011-2105), avec notamment, la nécessité de réduire de façon significative la pauvreté, et de faire du Sénégal un pays émergent. Le taux de croissance du PIB réel est projeté à 4,5% en 2011 contre 4,2% en 2010. Il devrait être porté par le dynamisme des secteurs primaire et tertiaire, ainsi que par la poursuite du redressement du Secteur secondaire :

- dans le secteur primaire, la croissance devrait ressortir à 3,8%
- s'agissant du secteur secondaire, il devrait enregistrer une progression de 5,1%
- et Concernant le secteur tertiaire, il devrait croître de 4,6% en 2011.

A cet effet, le gouvernement devra mettre en place des conditions propices au développement des différents secteurs économiques, notamment dans les secteurs de l'énergie et de la finance.

4.1 Historique de la SGBS

La création de la Société Générale remonte au 4 mai 1864, date du décret d'autorisation signé par Napoléon III. Forte de 140 ans d'histoire, la Société Générale a su se développer de façon considérable tant en France qu'à l'international. Le groupe Société Générale poursuit une politique de croissance rentable fondée sur un développement sélectif de ses produits et services, une innovation forte tournée vers la satisfaction de ses clients sur ses différents marchés, une croissance interne soutenue et quelques acquisitions ciblées.

La Société Générale est un des touts premiers groupe de services financiers de la zone euro, avec près de 151 000 personnes dans le monde.

Les équipes Société Générale proposent conseils et services aux particuliers, aux entreprises et aux institutionnels dans trois principaux métiers :

- la banque de détail en France avec les enseignes Société Générale, Crédit du Nord et Boursorama ;

- la banque de détail à l'international présente en Europe centrale & orientale et Russie, dans le bassin méditerranéen, en Afrique sub-saharienne, en Asie et en Outre-mer ;
- la banque de financement et d'investissement avec son expertise globale en banque d'investissement, financements et activités de marché ;
- la Société Générale est l'un des tous premiers groupes européens de services financiers. S'appuyant sur un modèle diversifié de banque universelle, le Groupe allie solidité financière et stratégie de croissance durable avec l'ambition d'être la banque relationnelle, référence sur ses marchés, proche de ses clients, choisie pour la qualité et l'engagement de ses équipes.

La SGBS au Sénégal a été créée exactement le 26/11/1962, avec un capital de 500.000.000 FCFA, et a connu un développement régulier au regard de l'évolution de son capital social :

Tableau 3 : Evolution du capital social

ANNEE	CAPITAL SOCIAL
1978	1.716.000.000
1979	2.156.000.000
1988	2.695.000.000
1989	3.234.000.000
1990	3.773.000.000
1993	4.312.000.000
1995	4.527.600.000
2008	10.000.000.000

Source : SGBS (2008)

La Société générale compte précisément 29 agences à Dakar et 14 autres dans les régions réparties entre : St louis , Louga , Touba , Mbacké , Diourbel , Thiès , Tivaouane , Rufisque , Saly portudal , Mbour , Kaolack , Kolda , Tambacounda et Ziguinchor.

A peu prés 3000 personnes travaillent à la Société Générale si on y ajoute le personnel exerçant dans les agences.

Le groupe compte principalement trois métiers régis directement par la maison mère à Paris (France).

Créée en janvier 2004, la branche Gestions d'actifs et Services aux investisseurs regroupe la Gestion d'actifs (Société Générale Asset Management), la Banque privée (SG Private

Banking), le métier Titres (Société Générale Securities Services) et la Banque directe (Boursorama) autour de 8.900 collaborateurs dans le monde. Le groupe Société Générale est la 4e banque gestionnaire d'actifs de la zone euro avec 397 milliards d'euros d'actifs gérés (à fin juin 2006) et le 3e acteur européen par les actifs en conservation avec 1516 milliards d'euros.

Selon la revue mensuelle « REUSSIR » n° 15 octobre 2007, la SGBS et la CBAO arrivent en tête du classement des banques en 2007 au Sénégal car chacun est premier à partir de l'un ou de l'autre critère essentiel. A savoir le total bilan pour la CBAO et le Produit Net Bancaire pour la SGBS.

En ce qui concerne le critère du total bilan, la CBAO dépasse la SGBS pour la première fois et arrive en tête avec 442,822 milliards contre 441, 360 milliards pour la SGBS.
En ce qui concerne le Produit Net Bancaire (le PNB), la SGBS devance la CBAO de plus d'un milliard (soit 29,6 milliards pour la Générale contre 28,5 milliards pour CBAO en 2005).
Par ailleurs la SGBS reste le principal financier de l'économie sénégalaise. En 2005 elle avait accordé 307 milliards de crédits soit une augmentation de 8 milliards entre 2005 et 2006.
Pour le critère du résultat net la SGBS arrive en tête avec 10, 143 milliards en 2006 contre 7, 485 milliards en 2005 (donc + 36 %).

4.2 Description du CSMM

Depuis 2001, les initiatives de normalisation, de mutualisation et de centralisation se sont multipliées au sein de BHFM. Le ralentissement de la croissance mondiale et l'augmentation de la pression concurrentielle imposent au Groupe Société Générale de poursuivre l'harmonisation de ses outils, ses processus et ses offres afin de produire les meilleurs services en réduisant ses coûts. Dans ce cadre, BHFM a initié, dans le courant de l'été 2009, le Programme de « Mutualisation Afrique », visant à mutualiser à l'horizon 2012 les fonctions support de 11 filiales d'Afrique subsahariennes. Chaque fonction support ayant pour vocation d'être regroupée dans un Centre de Services Mutualisés (CSM).

Face à la complexité des enjeux technologiques du système bancaire notamment la sécurisation des produits monétiques, la SGBS accueille, depuis mars 2010, le Centre de Services Mutualisés pour la Monétique (CSMM) en Afrique Subsaharienne.

Ce service à très forte valeur ajoutée, permet une gestion proactive complète. Il s'occupe entre autres, du traitement des opérations de Fraude, des Litiges, de la gestion des anomalies, des ajustages comptables monétiques, la télésurveillance des GAB etc.).

Dans le cadre d'une démarche globale de normalisation et de mutualisation, le pôle de la Société Générale chargé des réseaux internationaux, a commencé par centraliser les systèmes informatiques de ses onze filiales d'Afrique subsaharienne. La Société Générale choisit de regrouper trois fonctions support

- informatique,
- monétique et finance au sein de hubs régionaux.

Pour mener à bien ce projet complexe, à la fois technique, organisationnel et humain, la banque s'est appuyée sur l'expérience de CSC.
Lorsque la Société Générale décide de créer des centres de services mutualisés, son projet est encore très général, et elle souhaite l'aide d'un partenaire capable de l'épauler de bout en bout:

- définition de la structure ;
- mise en place des centres ;
- gestion du changement et pilotage du projet.

La banque choisit CSC, qui, non seulement, dispose d'un savoir-faire reconnu sur ce type d'opération et connaissait le contexte, mais surtout se présentait avec une équipe déjà constituée de professionnels aguerris. Créer de toute pièce une telle structure internationale requiert en effet un accompagnement expérimenté tant les sujets sont nombreux, complexes et nécessitent d'être abordés de façon approfondie. Immobilier, informatique, réglementation, fiscalité, plan de reprise d'activité : l'équipe projet, qui associe étroitement la Société Générale et CSC, ne devra rien laisser au hasard et ajuster les différents paramètres en tenant compte de l'hétérogénéité monétaire, fiscale et juridique de la région.

La répartition géographique des activités mutualisées a été définie en s'appuyant sur une analyse d'attractivité des différents pays d'implantation en Afrique subsaharienne. Les critères pris en comptes sont entre autres :

- la stabilité du pays ;

- la présence des autorités de régulation ;
- le dimensionnement du bassin d'emploi.

C'est dans cette optique qu'ont été créés les centres des services mutualisés monétique (CSMM), système d'information (CSMSI) et comptabilité-reporting (CSMCR).
Le CSM Monétique qui nous intéresse dans cette étude a d'abord démarré ses activités le 1er mars 2010 à Dakar pour un premier ensemble de filiales clientes. Un deuxième centre qui joue aussi le rôle de back up a été ouvert à Antananarivo en février 2012. La montée en charge du CSM Monétique est continuelle depuis sa création. Le centre compte à ce jour 34 collaborateurs répartis entre Madagascar et le Sénégal.
Le CSMM a repris partiellement ou totalement les activités des dix filiales que sont :

- la Société Générale de Banques au Sénégal ;
- la Société Générale Bénin ;
- la Société Générale Burkina Faso ;
- la Société Générale de Banques au Cameroun ;
- la Société Générale de Banques en Cote d'Ivoire ;
- la Société Générale Madagascar ;
- la Société Générale Mauritanie ;
- la Société Générale de Banques en Guinée ;
- la Société Générale de Banques en Guinée Equatoriale ;
- la Société Générale Tchad.

4.3 Objectif et enjeux du CSMM

4.3.1 Objectif

Le principal objectif du CSMM est de créer un pôle d'expertise Monétique basé à Dakar pour toutes les filiales d'Afrique sub-saharienne de la société générale.
L'atteinte de cet objectif permettra de :

- Accroitre les synergies commerciales régionales ;
- améliorer la qualité des services et le taux de satisfaction de la clientèle ;
- donner aux différentes filiales du réseau un accès à des compétences spécialisées et élargies ;

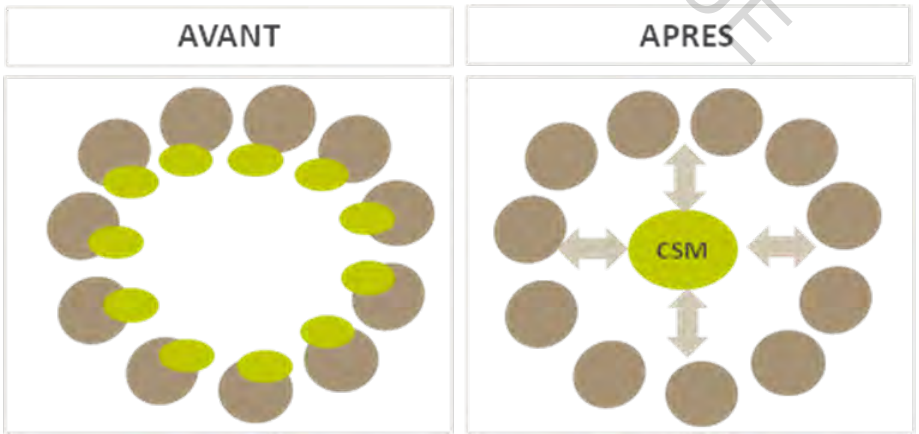
- mettre en place une organisation standardisée, assurant une meilleure maîtrise des risques opérationnels ;
- avoir une offre commerciale homogène et attractive ;
- développer une logique d'optimisation et de partage des coûts ;
- poursuivre la centralisation des infrastructures à mutualiser.

4.3.2 Enjeux du CSMM

Les enjeux pour le CSMM sont :

- Offrir une gamme de produits commerciaux élargie et identique à la clientèle de la zone ;
- atteindre et maintenir le niveau d'exigence Groupe quelle que soit la taille des filiales concernées ;
- mettre en place des solutions communes à l'ensemble des filiales concernées ;
- apporter des réponses rapides aux filiales de taille « sous-critique » ;
- standardiser les outils et processus ;
- mettre en œuvre la mobilité régionale ;
- favoriser le développement des compétences et des talents de la zone ;
- accélérer l'intégration et la valorisation de toute nouvelle acquisition.

Figure 5 : Représentation schématique de la mutualisation



Source : **CSMM (2010)**

4.4 L'organisation et les activités du CSMM

Comme le montre l'organigramme en annexe 3, le CSMM est composé, en plus de la direction générale, de quatre pôles que sont :

- le pôle projet ;
- le pôle offre monétique ;
- le pôle opérations et le pôle assistance ;
- une assistante de direction.

4.4.1 Le pôle projet

Le pôle projet s'occupe entre autres de :

- la gestion des projets ;
- la mise en œuvre et l'accompagnement au déploiement ;
- la qualification de la demande.

4.4.2 Le pôle offre monétique

Le pôle offre monétique avec ses 2 collaborateurs a des activités qui tournent autour du :

- développement de l'offre monétique ;
- développement de la relation avec les fournisseurs.

Au sein du pôle opérations, les activités tournent autour des grands axes que sont :

- les ajustements comptables ;
- les litiges ;
- la fraude ;
- la gestion et la qualification des anomalies.

Les collaborateurs du pôle assistance ont des activités qui se résument en :

- la gestion des demandes des porteurs de carte ;
- la télésurveillance des DAB ;
- la gestion des demandes des commerçants ;

- la gestion de la demande des conseillers clientèle ;
- la qualification et la gestion des investigations.

Il faut noter qu'une équipe de nuit est présente de 17h à 7h pour assurer la continuité de ce service 24h/24.

Conclusion Chapitre 4

Qu'il s'agisse de la conduite du changement auprès des filiales ou du recrutement des personnels des centres, la Société Générale et CSC ont travaillé en parfaite symbiose pour n'omettre aucun détail. Le centre monétique de Dakar qui débute son activité, a été suivi par le centre d'exploitation informatique de Dakar, dont le pendant pour la zone Afrique centrale ouvre à Douala. À Douala également, le centre de service mutualisé finance est pour sa part opérationnel. Le lancement rapide d'une nouvelle carte de paiement par la monétique illustre parfaitement les bénéfices de la mutualisation, qui offre plus de réactivité et de moyens pour mieux servir les filiales et leurs clients.

CHAPITRE 5 : ACTIVITES DU CSMM ET APPLICATION DES NORMES

Introduction

Nous vous expliquerons ici comment fonctionne le CSMM et quelles sont les activités qui y sont menées. Avant de nous pencher sur la phase descriptive des différentes taches, nous parlerons de la gestion du CSMM et ensuite nous vous montrerons comment se font le choix et le transfert des activités monétiques. Ce choix consiste à définir quelles sont les tâches qui incombent au CSMM et quelles sont les tâches qui restent au niveau des filiales.
Nous vous montrerons par la suite qu'est ce qui est fait dans chaque pôle. Une attention particulière sera portée au pôle opération dans lequel nous exerçons notre activité.
C'est par la suite que nous verrons comment et à quel point les normes internationales sont appliquées au niveau du CSMM et des filiales qu'il gère.

5.1 La gestion du CSMM :

Le CSMM n'est pas une entité juridique pure et à part entière. Il dépend hiérarchiquement de la BHFM et de son entité Afrique Moyen Orient. Il dépend fonctionnellement de la monétique du siège du groupe et administrativement de la SGBS qui est la filiale qui l'héberge.

Ce choix de rattacher le CSMM administrativement à la SGBS et de le faire héberger par cette dernière a été fait pour soucis de simplicité et pour rendre l'implantation du CSMM plus facile et moins lourd. Le CSMM utilise donc tous les moyens généraux de la filiale sans frais particuliers à part les charges comme la location, l'électricité. La comptabilité est gérée au niveau de la SGBS comme si le CSMM était une agence. Cependant, après les imputations comptables, tout est envoyé au CSMM pour vérification et c'est par la suite que le CSM Comptabilité-reporting qui s'occupe du suivi budgétaire.

Le CSMM entretient une relation « prestataire de service-client » avec les filiales dont elle a repris l'activité. C'est en fonction des activités reprises pour chaque filiale que la facturation est faite. Ceci consiste généralement à répartir le coût des ressources utilisées pour réaliser chaque activité.

Plusieurs outils sont utilisés par les dirigeants du CSMM pour mesurer sa performance. Il y a d'abord les indicateurs clés de succès (KPI) mais surtout la SLA (Service Level Agreement) qui est une sorte de convention de service et qui définie la qualité de service requise entre le prestataire qu'est le CSMM et le client qui est la filiale. En guise d'exemple, on peut citer le fait que le CSMM s'engage au niveau de la gestion des litiges à ne perdre aucun litige ou au niveau du centre d'appel à faire en sorte que le taux d'échec des appels soit de moins de 20%.

5.2 Transfert de l'activité monétique du CSMM

Le transfert de l'activité permet de prendre une partie des activités monétiques que la filiale assurait pour les confier au CSMM sans pour autant freiner ou apporter un dysfonctionnement au niveau de la monétique de la filiale.

Pour y arriver, le CSMM dispose de ce qu'on appelle le « Kit de reprise ». Ce Kit permet dans les grandes lignes de :

- présenter le CSMM, son objectif, son fonctionnement ;
- définir les activités qui sont reprises par le CSMM ;
- définir les activités qui restent en filiale ;
- décomposer le mode de fonctionnement de la filiale d'en avoir une vision plus net et arranger les imperfections ou les points qui doivent être améliorés.

Les activités monétiques peuvent se résumer à la liste ci-dessous :

- les projets avec la gestion opérationnelle des projets ;
- les anomalies avec l'identification des anomalies monétiques dans les outils existants, la remontée au siège, le suivi de leur résolution ;
- les litiges qui concernent le traitement des réclamations clients sur les transactions, le suivi des chargebacks avec les réseaux internationaux (VISA, Mastercard,…) ;
- la fraude (prévention et détection de la fraude externe grâce aux modèles de comportements frauduleux en place) ;
- la télésurveillance (surveillance à distance et en temps réel du bon fonctionnement des DAB/GAB) ;
- l'assistance (l'assistance aux agences sur les aspects monétiques, assistance commerçants, assistance porteur) ;
- le reporting (reporting réglementaire et de suivi de l'activité) ;

- les ajustements comptables (le rapprochement des états VISA et Mastercard, identification d'écarts et préparation des écritures comptables à saisir dans l'outil comptable) ;
- la comptabilité monétique (la saisie des écritures comptables dans l'outil comptable) ;
- la gestion des contrats monétiques (création et modification des contrats porteurs et commerçants) ;
- la logistique cartes (renouvellement/ annulation de cartes, modification de PIN, suivi des stocks, dispatching dans les agences) ;
- les activités dabistes (remplissage des DAB, support à la mise en place des DAB, ajustements comptables portant sur les DAB) ;
- les activités technico-commerciales (assistance au Réseau pour la vente aux commerçants, assistance TPE).

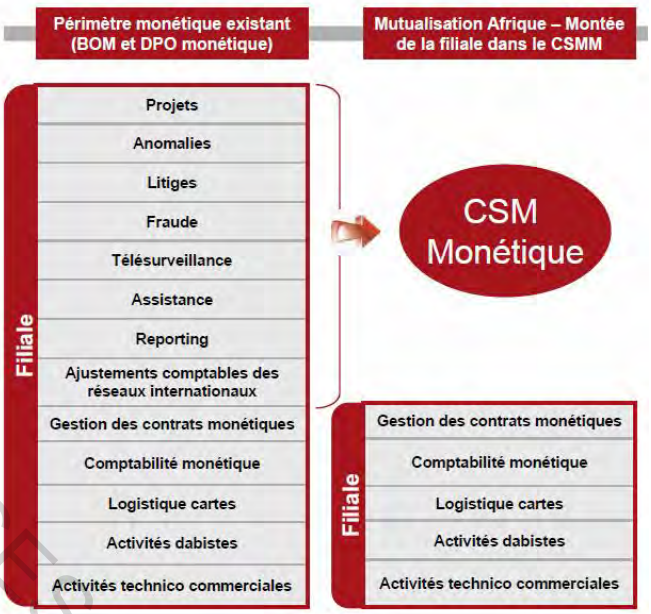
Une partie de ces activités est par la suite reprise et gérée par le CSMM. Il s'agit de :

- les projets ;
- la gestion des anomalies ;
- la gestion des litiges;
- la gestion de la fraude;
- la télésurveillance;
- l'assistance;
- le reporting;
- les ajustements comptables monétiques.

Les autres activités (nous avons essayé de les présenter plus haut en intégralité) restent à la charge des filiales.

Le schéma ci-dessous montre la relation entre le CSMM et les filiales et nous présente une vision des activités mutualisées et des activités qui restent en filiales.

Figure 6 : Répartition des activités du CSMM et ses filiales



Source : CSMM (2010)

5.3 Fonctionnement des pôles

5.3.1 Le pôle projet

Ce pôle est composé du responsable des projets et de 5 chefs de projets.

Leurs principaux rôles sont :

- coordonner les projets, une coordination qui se fait du lancement du projet jusqu'à la mise en production c'est-à-dire quand tout est opérationnel. Les chefs de projets sont les intermédiaires entre les filiales, les processeurs, les prestataires, etc. Ils s'assurent que tout se passe bien et que tout est pris en compte techniquement ;
- mener à bien les projets confiés dans le cadre de la stratégie du groupe Société Générale et des décisions validés au sein des filiales ;
- veiller au bon respect des délais et budgets impartis ;
- jouer le rôle de superviseurs des filiales en étant l'interlocuteur direct des filiales pour les questions relevant de la monétique mais surtout des aspects techniques. Par exemple lors de l'acquisition d'un matériel, les chefs de projets sont sollicités pour faire les vérifications techniques et tarifaires nécessaires avant de donner leur accord.

Parmi les projets phares réalisés par ce pôle, nous pouvons citer l'acquisition MasterCard, la migration vers la norme EMV, et l'ouverture de certains nouveaux réseaux comme CUP et AFFN.

5.3.2 Le pôle assistance

Le pôle assistance s'occupe de :

- la gestion des demandes des porteurs de carte qui peut s'agir d'une demande de mise en opposition pour un client qui a perdu sa carte bancaire ; d'une demande d'augmentation de plafond ; d'une demande de réinitialisation de code ; d'une demande d'information sur une carte qui ne fonctionne pas ; etc. ;
- la télésurveillance des DAB, le CSMM dispose d'un outil nommé Dispatch Manager qui lui permet de savoir à temps réel l'état des distributeurs automatiques de billet. Lorsqu'il y a un problème quelconque sur un distributeur donné, l'agent devant son ordinateur le voie et décide de la démarche à tenir. Il peut soit redémarrer le distributeur surplace à partir de son ordinateur soit envoyer un email à qui de droit pour lui demander d'agir de manière approprié afin de permettre au DAB de fonctionner correctement et d'éviter qu'il ne soit à l'arrêt. Ce service fourni par le CSMM assure aux filiales l'augmentation du taux de disponibilité de leurs DAB et l'augmentation de la qualité de service ;
- la gestion des demandes des commerçants pour une demande d'autorisation concernant une transaction, d'une action à mener sur un TPE ;
- la gestion de la demande des conseillers clientèle, le pôle assistance répond aux conseillers clientèles sur toute question concernant la monétique, les procédures, les demandes de recherches, les demandes d'opposition ;
- la qualification et la gestion des investigations, il s'agit ici de recherches ou d'investigations menées pour pouvoir dénouer un désaccord ou un litige ou tout simplement pour permettre une meilleure prise en charge de la réclamation d'un client. Certains cas ne pouvant pas être réglés au téléphone car nécessitant une investigation plus poussée sont confiés à ceux qui s'occupent des investigations.

Les clients, commerçants et conseillers clientèles disposent d'un numéro où ils peuvent appeler 24h/24 pour que quelqu'un puisse s'occuper de leur demande. C'est un pôle qui est en contact permanent avec les différents utilisateurs des produits monétiques des filiales.

5.3.3 Le pôle développement de l'offre monétique

C'est un pôle dont la création est récente et qui répond au souci d'apporter une valeur ajoutée, un plus à la filiale.

Il a pour rôle de réfléchir en amont sur les nouveaux projets ; de faire les études d'opportunité ; de développer et de promouvoir de nouvelles offres monétiques.
Un des agents de ce pôle est spécialement en charge de la relation fournisseurs, il participe aux négociations, assure un suivi des commandes. Il s'occupe aussi du développement commercial et du suivi de l'activité monétique des filiales.

Ce pôle fait aussi du conseil en donnant aux filiales des orientations et assure la veille technologique et concurrentielle tout ceci dans le but d'améliorer l'offre proposée aux clients, leur apporter une solution adaptée aux problèmes rencontrés, améliorer et optimiser les relations avec les fournisseurs.

Comme réalisations de ce pôle, nous pouvons citer :

- La réalisation de la note d'opportunité des cartes prépayés qui a portée sur l'analyse des cartes prépayées Visa, MasterCard et GIM-UEMOA et la recommandation du CSMM d'émettre des cartes prépayées Mastercard ;
- la réalisation de la note d'opportunité du réseau SG Afrique qui porte sur la mise en place d'un réseau privatif pour toutes les filiales gérés par le CSMM à l'image des réseaux internationaux tels que Visa et Mastercard.

5.4 Le pôle opérations

Selon GIM-UEMOA (2007) c'est dans ce pôle et sous la responsabilité du responsable des opérations qu'est géré l'ensemble des activités opérationnelles notamment les ajustements comptable, la fraude, les anomalies, les chargebacks.

Sa mission première est de suivre, détecter, analyser, traiter toutes opérations afin de garantir le bon fonctionnement de l'activité monétique des filiales. La mutualisation des activités back

office des filiales a permis une prise en charge effective et efficiente des opérations quotidiennes par des ressources spécialisées.

Aujourd'hui, toutes les filiales disposent des mêmes services avec les mêmes capacités de réaction et d'intervention. La prise en charge de ces activités par ce pôle permet l'harmonisation des procédures de traitement des opérations et surtout l'intégration de nouveaux réseaux sans impact sur les ressources humaines des filiales.

5.4.1 Les ajustements comptables

Les ajustements comptables consistent à faire les rapprochements des états des opérateurs internationaux (VISA, MASTERCARD, CUP,…), à identifier les écarts et à préparer les écritures comptables à saisir dans l'outil comptable.

Nous prendrons ici l'exemple d'une filiale comme la SGBS. Le principe est le suivant :

- des porteurs de cartes de la SGBS vont au niveau des autres banques à l'étranger ou chez les confrères pour effectuer des transactions retraits ou achats avec leur carte bancaire. Ce sont les transactions émissions ;
- des porteurs de cartes des autres banques viennent au niveau des distributeurs de la SGBS ou chez des commerçants de la SGBS pour effectuer des transactions. Ce sont les transactions acquisitions ;
- pour chaque journée, les réseaux internationaux (VISA, MASTERCARD,…) par lesquels ces transactions transitent font la compensation entre les transactions émissions et les transactions acquisition pour sortir le montant de la couverture. Si le montant des transactions acquisition est supérieur que le montant des transactions émission, la compensation sera créditrice et si le montant des transactions émission est supérieur au montant des transactions acquisition, la compensation sera débitrice ;
- un état récapitulatif est alors envoyé par ces réseaux à la SGBS avec le montant de la couverture attendue qui sera débité ou crédité du compte de la SGBS. Cet état contient aussi le montant des frais et charges supportés, le montant des commissions reçues, et les détails des transactions.

Chaque filiale reçoit cet état récapitulatif. Le service ajustement comptable utilise donc cet état pour préparer un document pré-rempli appelé fiche d'ajustage. Cette fiche relate chaque

type de transaction qui a eu lieu de même que les commissions et charges. Ce document est envoyé à la filiale qui prépare une pièce comptable pour régulariser les opérations en suspens sur sont compte.

Ce travail de rapprochement est fait pour chaque filiale et pour chaque réseau. En plus de cela, les agents chargés des ajustements comptables ont pour rôle de répondre aux demandes d'information de la filiale concernant les opérations en suspens, la surveillance des comptes sensibles, la facturation mais aussi, plus généralement, toute demande de la filiale qui relève de leur compétence.

5.4.2 La gestion des litiges

La gestion des litiges est faite par deux équipes : une qui s'occupe des chargebacks et une autre qui s'occupe de la fraude. Ce sont deux activités sensibles qui demandent beaucoup d'attention et un suivi minutieux pour éviter des pertes considérables pour les filiales.

5.4.2.1 La gestion des chargebacks

Un chargeback a lieu quand le titulaire de la carte informe sa banque qu'une transaction n'avait pas été autorisée par lui ou que le produit commandé par lui n'a pas été livré. En d'autres termes, il s'agit d'un impayé car le vendeur devra rembourser le porteur de la carte.
Il existe plusieurs niveaux de chargebacks, les plus graves étant pour fraude, ou lorsque la carte a été volée.

Les sociétés de paiement en ligne et banques partenaires ont du mal à tolérer plus de 1% de chargebacks frauduleux, sans quoi les comptes marchands sont fermés par les réseaux des cartes bancaires, d'où l'importance des sociétés telles que Cashtronics qui offrent des solutions anti-fraude performantes. D'abord, en guise d'éclaircissement, on peut dire qu'un chargebacks est une contestation d'une opération effectuée par un porteur.

Un chargeback survient quand le titulaire de la carte informe sa banque qu'une transaction n'avait pas été autorisée par lui ; que le produit commandé par lui n'a pas été livré ou que l'argent demandé au niveau du GAB n'est pas distribué. En d'autres termes, il s'agit d'un impayé.

5.4.2.2 La gestion de la fraude

L'activité de gestion de la fraude consiste à la prévention, à l'identification et à la détection de la fraude afin de protéger les filiales. C'est une activité très sensible quand on considère les conséquences qu'une fraude peut avoir.

La détection peut se faire soit par l'intermédiaire des clients et agences qui donnent l'alerte, soit par l'intermédiaire de l'agent chargé de la gestion de la fraude à la suite des analyses qu'il effectue sur les transactions d'une filiale donnée. Mais les rôles principaux des agents chargés de la fraude sont de :

- concevoir et de mettre en œuvre les outils de gestion de la fraude ;
- analyser les transactions et alerter la filiale en cas de suspicion de fraude ;
- faire de la veille technologique par rapport aux tendances de la fraude.

Des actions adéquates sont par la suite menées conjointement entre le CSMM, la filiale et les réseaux internationaux sur lesquels la fraude se passe.

Une nouvelle solution de gestion de la fraude est en cours de mise en place. Elle permettra de diminuer les pertes opérationnelles dues à la fraude ; d'accroitre la réactivité du CSMM face à tout nouveau risque de fraude ; de suivre la pertinence des règles anti-fraude au moyen d'indicateurs ; de réagir en temps réel ; de faciliter l'instruction des dossiers par le backoffice.

5.4.3 La gestion et la qualification des anomalies

La mission principale des agents chargés de la gestion des anomalies et d'accompagner et suivre la résolution des problèmes de fonctionnement que lui communique les filiales ou les autres services du CSMM.

Pour mener à bien cette mission, lorsqu'on leur communique une anomalie sur le système d'information monétique les tâches effectuées sont généralement d'analyser le dysfonctionnement en fonction des informations reçues puis d'évaluer le type de

dysfonctionnement. Ces dysfonctionnements peuvent venir d''un problème technique ou d'une mauvaise utilisation du système d'information.

Les actions adéquates sont par la suite entreprises pour résoudre le problème. Si c'est un problème lié à une mauvaise utilisation du système d'information, une communication est transmise afin d'aider à une meilleure utilisation de l'outil. Si c'est un problème d'ordre technique, une fiche de résolution de l'anomalie est rédigée et l'agent suit la résolution du problème avec le processeur du CSMM.

C'est un service qui occupe une place importante vues les différentes sortes d'anomalies qui peuvent survenir dans le système d'information monétique et les conséquences que ces anomalies peuvent entrainer.

5.5 Application des normes EMV par CSMM et ses filiales

5.5.1 Les cartes bancaires

La migration des cartes à pistes qui existaient vers des cartes à puce qui respectent les normes EMV a commencé en 2011 et se poursuit toujours. Cette migration consiste à remplacer les cartes à piste par des cartes à puce.
Il y a eu deux cas. Le premier est pour les nouvelles cartes fabriquées pour les nouveaux clients. Ces cartes étaient systématiquement des cartes à puce, c'est-à-dire qu'elles sont fabriquées en respectant les normes EMV. L'autre cas consistait à remplacer les cartes arrivées à expiration par des cartes à puce.
Cette migration n'a pas concerné toute, la gamme de carte de toutes les filiales. Le tableau ci-dessous liste la gamme de carte par filiale et les cartes qui sont à puce ou non.

Tableau 4 : Les différents types de cartes des filiales gérées par le CSMM :

Banque	Pays	Produits actuels			Respect de la norme EMV
		Type de carte	Mode de traitement	Nom de la carte	
BFVSG	Madagascar	Privative	Piste	Salaire	NON
		Privative	Piste	Eclair	NON
		Privative	Piste	Poinsettia	NON
		VISA	EMV	Electron Varongy	OUI
		VISA	EMV	Classic Ebène	OUI
SGB	Bénin	Privative	Piste	Salaire	NON
		Privative	Piste	Eclair	NON
		VISA	EMV	Classic	OUI
		VISA	EMV	Electron	OUI
		VISA	EMV	Business silver	OUI
SGBB	Burkina Faso	Privative	Piste	Salaire	NON
		Privative	Piste	Hibiscus	NON
		VISA	EMV	Electron Salaire	OUI
		VISA	EMV	Classic	OUI
		VISA	EMV	Electron	OUI
		VISA	EMV	Gold	OUI
SGBC	Cameroun	Privative	Piste	Salaire	NON
		Privative	Piste	Privilège	NON
		Privative	Piste	Préférence	NON
		VISA	EMV	Business	OUI
		VISA	EMV	Electron	OUI
		VISA	EMV	Electron - Visa prépayée	OUI
		VISA	EMV	Classic	OUI
		VISA	EMV	Premier	OUI
		Privative	Piste	Advans [carte cobrandée]	NON
		VISA	EMV	Electron - Package Easy	OUI
SGBCI	Côte d'Ivoire	Privative	Piste	Salaire	NON
		Privative	Piste	Eclair	NON
		VISA	EMV	Business	OUI
		VISA	EMV	Electron	OUI
		VISA	EMV	Classic	OUI
		VISA	EMV	Classic Etudiant	OUI
		VISA	EMV	Premier	OUI
SGBG	Guinée	Privative	Piste	Eclair	NON
		Privative	Piste	Salaire	NON

		Privative	Piste	Sago	NON
		VISA	EMV	Classic	OUI
		VISA	EMV	Gold	OUI
		VISA	EMV	Business	OUI
SGBGE	Guinée Equatoriale	Privative	Piste	Express	NON
		Privative	Piste	Salaire	NON
		VISA	EMV	Classic	OUI
		VISA	EMV	Gold	OUI
SGBS	Sénégal	Privative	Piste	Azur [Epargne]	NON
		Privative	Piste	Azur [Epargne]	NON
		Privative	Piste	Salaire	NON
		Privative	Piste	Salaire	NON
		VISA	EMV	Classic débit immédiat	OUI
		VISA	EMV	Classic débit différé	OUI
		VISA	EMV	Classic Business	OUI
		VISA	EMV	Premier débit immédiat	OUI
		VISA	EMV	Premier débit différé	OUI
		VISA	EMV	Carte Premier Business	OUI
		VISA	Piste	Premier Business	NON
		VISA	EMV	Electron	OUI
SGM	Mauritanie	Privative	Piste	Silver	NON
		Privative	Piste	Gold	NON
		Privative	Piste	Salaire	NON
		VISA	EMV	Classic	OUI
		VISA	EMV	Business Gold	OUI
SGT	Tchad	Privative	Piste	SGTB	NON
		Privative	Piste	Privilège	NON
		Privative	Piste	Salaire	NON
		VISA	EMV	Business	OUI
		VISA	EMV	Classic	OUI
		VISA	EMV	Premier	OUI

Source : CSMM (2010)

5.5.2 Les TPE et les GABs :

Tout le parc TPE des filiales que le CSMM gère est EMV. Les TPE acceptent les paiements par carte à puce. Il est difficile de donner le nombre exact de TPE puisque y en a qui sont dans le réseau ou chez les commerçants et qui sont inactifs ou hors service. Il faut noter aussi que même si les TPE sont EMV, les commerçants peuvent avoir recours à des facturettes quand le TPE a des problèmes. Le principe des facturettes consiste à copier sur une feuille les données de la carte et e montant de la transaction. Cette feuille est ensuite envoyée au service

monétique qui va saisir dans un logiciel ces données. Le montant de la transaction sera par la suite débité du compte du client et crédité dans le compte du commerçant. Le principal fournisseur de TPE des filiales est INGENICO.

Les GAB des filiales sont tous EMV comme c'est le cas des TPE. Mais il est possible que lorsqu'un porteur se présente avec sa carte à puce et que la puce rencontre un petit problème ou un disfonctionnement, le GAB va lire la piste comme si ce n'est plus EMV. Les principaux fournisseurs GAB avec lesquels le CSM travaille sont Diebold, NCR et Wincor.
Le tableau ci-dessous fait récapitule le nombre de GAB par filiale.

Tableau 5 : Nombre de GAB par filiale

FILIALES	Nombre de GAB			
	NCR	Wincor	Diebold	Total
SG BENIN	15	0	2	17
SG BURKINA	7		12	19
SGBC	14	20	6	40
SGBCI	15	0	77	92
SGBG	0	17	0	17
SGBGE	0	7	0	7
BFV –SG	35	17	0	52
SGM	3	20	0	23
SGBS	56	0	1	57
SGT	0	17	0	17
SGC	2	0	0	2
TOTAL	147	98	98	343

Source : CSMM (2010)

5.6 Application des normes PCI

L'élément central et déterminant de cette norme est le numéro de la carte. La norme EMV s'applique uniquement si les PAN sont stockés traités ou transmis. Elle s'applique donc à tous les niveaux et toutes les entités qui sont concernés dans le circuit de stockage, de traitement et de transmission du numéro de carte.

Pour décrire la manière dont les normes PCI sont appliquées et leur niveau d'application, nous ferons un tableau qui a été effectué en exploitant les réponses obtenues lors des entretiens qui avaient pour but de vérifier si les différentes conditions de la norme sont prises en compte. Lors de ces entretiens, un questionnaire a été soumis aux personnes concernées. Ce questionnaire se trouve en annexe 4. Nous avons aussi eu recours à l'observation pour en savoir plus et faire une confrontation. Ceci nous a permis de mettre en œuvre le tableau de synthèse ci-dessous.

Tableau 6 : Niveau d'application des conditions de la norme PCI

Condition	Appliquée	Appliquée en partie	Pas appliqué
Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes	X		
Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur		X	
Protéger les données de titulaires de cartes stockées		X	
Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts		X	
Utiliser des logiciels antivirus et les mettre à jour régulièrement	X		
Développer et gérer des systèmes et des applications sécurisés	X		
Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître		X	
Affecter un ID unique à chaque utilisateur d'ordinateur	X		
Restreindre l'accès physique aux données des titulaires de carte	X		
Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de carte			X
Tester régulièrement les processus et les systèmes de sécurité	X		
Gérer une politique de sécurité des informations pour l'ensemble du personnel	X		

Source : CSMM (2010)

Conclusion chapitre 5

La description de l'activité de CSMM nous permettra de mettre en relief les points de faiblesses relatifs :

- aux conditions d'utilisation de la carte bancaire ;
- à la sécurisation des installations ;
- au respect des normes ;
- à l'organisation du CSMM.

Le chapitre suivant va faire l'analyse de ses faiblesses ci-dessous et essayer de faire des recommandations pour la résolution de ces faiblesses.

CHAPITRE 6 : ANALYSE ACTIVITE DU CSMM ET RECOMMANDATIONS

Introduction

L'analyse des données de CSMM se basera essentiellement sur le modèle d'analyse établi au chapitre 3.

Ainsi nous analyserons :

- le niveau d'application des normes et bonne pratiques au CSMM ;
- la gestion de la monétique au sein du CSMM ;
- la gestion des ressources humaines au CSMM
- le niveau d'application des normes PCI et EMV ;

La description de l'activité de CSMM nous avait permis de voire d'un premier abord des faiblesses. L'analyse de ces faiblesses sera aussi faite afin de trouver des solutions que nous exposerons plus tard. Ses faiblesses sont relatives:

- aux conditions d'utilisation de la carte bancaire ;
- à la sécurisation des installations ;
- au respect des normes ;
- à l'organisation du CSMM.

Des recommandations seront par la suite émises par rapport aux constats de notre analyse tout ceci dans le but d'améliorer le fonctionnement et l'apport du CSMM.

6.1 Analyse des pratiques du CSMM

Pour mener à bien cette analyse, nous nous sommes mis aussi bien du coté de la filiale que du coté du CSMM et de BHFM. Nous avons aussi cherché les apports du CSMM sur le plan organisationnel, commercial. Nous nous sommes surtout penchés sur les plus-values d'une telle structure. Nous avons ensuite fait le point sur l'application des normes.

6.1.1 Les apports du CSMM sur la gestion de l'activité monétique des filiales :

Ce qui est principalement recherché au CSMM est l'optimisation des ressources, l'harmonisation et la qualité de service ; tout ceci à moindre coût. Le CSMM se pose comme point de contact entre BHFM et les filiales. Sur un plan plus large, le CSMM représente les filiales au sein des organismes régionaux comme GIM-UEMOA et internationaux comme VISA et Mastercard. Tout ceci permet de simplifier la relation que ces différents acteurs ont avec les filiales.

Les capacités de négociation et de lobbying sont encore plus développées avec l'approche communautaire prise par ce projet. Par exemple, le CSMM a pu imposer à certains fournisseurs de revoir les prix des GAB. Il se trouve que certains fournisseurs vendaient les distributeurs à un prix très élevé à certaine filiales. Le cas peut être illustré par un constructeur de distributeur automatique de billet qui avait un produit vendu environ 10 millions FCFA à la filiale du SENEGAL alors que ce même distributeur automatique de billet pouvait être vendu 50% plus cher à la filiale du Cameroun ou du Congo. Vu le nombre de filiales et le nombre de distributeurs automatiques de billets susceptibles d'être achetés dans tout le réseau Société Générale d'Afrique Subsaharienne et de Madagascar, les fournisseurs n'hésitent plus à baisser considérablement les prix et surtout à les harmoniser d'un pays à l'autre pour espérer vendre un maximum de produits. De plus, lors des négociations, ils font face cette fois-ci à des professionnels très expérimentés qui n'accepteront pas des prix très élevés et injustifiés.

C'est une nouvelle expérience pour le groupe Société Générale car il n'y avait pas auparavant des centres de ce type. Certains établissements financiers ont certes des centres de traitement monétiques depuis peu, mais le modèle reste différent. Les centres de traitement dont nous parlons n'ont pas les différents pôles proposés par le CSMM. C'est la première fois que ce modèle de gestion est expérimenté. C'est aussi la première fois que la banque fait recours à de vrais contrats d'expatriation Afrique-Afrique.

Grace au CSMM, la filiale bénéficie:

- d'une réorganisation de l'activité monétique : puisqu'une partie des activités est reprise par le CSMM, la filiale devra réorganiser le service monétique en fonction des activités restantes afin d'optimiser les ressources et le temps de travail. Les filiales

pourront donc se concentrer beaucoup plus sur la relation clientèle, sachant que tout l'aspect technique et support est pris en charge au CSMM ;

- d'une mise à niveau des processus monétiques au sein de la filiale pour fluidifier les échanges avec le CSMM et tendre vers l'organisation cible des filiales d'Afrique subsaharienne. Avec les standards voulus par le CSMM et vu que le CSMM restera le principal interlocuteur des filiales pour les questions relevant de la monétique, une mise à niveau s'impose au sein de certaines filiales afin de faciliter la collaboration entre les deux entités. Cette standardisation permettra aussi de limiter ou de maitriser les risques opérationnels et les coûts. Il faut noter que chaque filiale avait ces propres pratiques et ses propres processus ;

- d'une réaffectation des ressources humaines libérées lors du processus de transfert de certaines activités de la filiale au CSMM car ce transfert entraine la libération de certains agents. Ces derniers seront donc réaffectés dans les autres services de la banque ce qui peut être bénéfique pour la filiale. Ceci représente d'une certaine manière une opportunité pour ces gens qui sont réaffectés à d'autres tâches. La filiale en profite aussi pour disposer de ressources humaines supplémentaires sans avoir besoin de recruter ;

- d'une mise à disposition de compétences spécialisées quelle que soit sa taille. Avant le CSMM, certaines filiales disposaient d'un spécialiste dans un domaine de la monétique et d'autres pas. Certaines compétences étaient donc inexistantes dans certaines filiales. Les filiales les plus en avancées côté monétique étaient la SGBS, la SCBCI et le BFV-SG. Avec le regroupement des experts et spécialistes dans un centre au service de toutes les filiales, ces dernières pourront toutes profiter des compétences en place. Nous pouvons donner l'exemple du déploiement rapide d'un peu moins d'une dizaine de réseaux (VISA, Mastercard, CUP, AFFN, PULSE, GIM, American Express,etc.) dans toutes les filiales. Toutes les filiales de toutes les pays ont pu prendre de l'avance par rapport à la concurrence. Vous avez ci-dessous un tableau montrant la disponibilité des différents réseaux par rapport aux autres banques des autres pays ;

Tableau 7 : tableau de comparaison sur la disponibilité des différents réseaux :

Réseau	Disponible dans toutes les filiales ?	Disponible certaines banques des autres pays ?
VISA	Oui	Oui
Mastercard	Oui	Oui
CUP	Oui	Non
AFFN	Oui	Non
AmEx	Oui	Oui
GIM	Oui	Non
Pulse	oui	Non

Source : CSMM (2010)

- la disponibilité 24h/24 du call center est une nouveauté que les filiales voir même les autres banque de la zone ne pouvait pas avoir. La disponibilité du call center est aussi un des points forts du CSMM.

Dans une autre mesure, la Société Générale pourra développer une offre commerciale homogène et attractive au sein de toutes ces filiales. Il faut aussi considérer en dehors de cette harmonisation, il y a un intérêt économique car les coûts de pilotage et d'exploitation seront partagés entre les filiales. Par exemple, pour un projet donné, les frais pour les tests se feront pour une seule filiale, et dès que les tests sont concluants, le projet est adapté aux autres filiales.

L'expérience du CSMM a aussi montré qu'avec cette formule de mutualisation, il y a une meilleure prise en charge des projets monétiques. Les filiales bénéficient de ce qu'on peut appeler des projets « clés en main ». Tout est géré au niveau du CSMM. La filiales n'aura pas besoin de payer des experts, d'envoyer ses agents en formation, de recruter, de bouleverser son fonctionnement etc. ceci étant une plus value non négligeable. La mise en place de nouveaux réseaux ou de nouveaux projets est directement traitée au quotidien par le CSMM. La filiale ne se contentera par la suite que de communiquer et d'entreprendre des actions marketing nécessaires au développement du nouveau produit.

En plus du coté purement technique et opérationnel, la création récente d'un pole développement de l'offre monétique démontre la volonté des dirigeants du CSMM d'apporter continuellement un plus, une valeur ajoutée afin de développer la monétique au sein des filiales. Ceci permettra continuellement aux filiales de commercialiser des produits qu'elles n'avaient pas.

6.1.2 La gestion des ressources humaines au CSMM

Il est important d'analyser ce point car c'est ce qui fait la réussite du CSMM. Nous avons dit plus haut que c'est la première fois que le groupe Société Générale fait recours à de vrais contrats d'expatriation Afrique-Afrique. Le centre a regroupé la majorité des responsables monétique des filiales pour les amener à Dakar et Antananarivo afin de répondre aux besoins des filiales. Le principal challenge était d'entreprendre et de réussir les contrats d'expatriations Afrique-Afrique. C'est-à-dire des agents de la Société Générale d'une filiale africaine qui sont envoyés en expatriation dans un autre pays où est implanté la Société Générale, toujours en Afrique. Avant le CSMM, l'expatriation se faisait soit d'Europe vers l'Afrique ou de l'Afrique vers l'Europe. Donc c'est un modèle nouveau qu'il a fallu mettre en place avec une équipe RH ambitieuse et expérimenté afin de s'assurer que tous les facteurs sont pris en charge pour que l'expatriation se passe dans les meilleures conditions.

Tout ceci à pu aussi se faire avec l'aide le la filiale locale c'est-à-dire la SGBS qui à mis tous les moyens nécessaires (aussi bien humains que matériels) à la disposition du CSMM et de ses expatriés.

L'autre côté positif a été le fait que différents entretiens ont été effectués sur le plan local afin d'identifier les meilleurs agents de la SGBS à affecter au CSMM.

Cette gestion des ressources humaines est l'hune des clés de réussite du projet.

6.1.3 Le niveau d'application des normes PCI et EMV

- La norme EMV

L'analyse des données recueillies nous montre que 100% des TPE et des DAB des filiales gérées par la CSMM sont EMV. Ceci protège la Société Générale en partie contre le transfert de responsabilité en cas de fraude concernant les cartes des banques confrères ou étrangères qui effectuent des transactions sur le réseau Société Générale.

Par contre, les informations recueillies lors de certains entretiens ont permis de nous rendre compte que même si les TPE et DAB sont EMV, elles font des transactions en fall-back. Le fall-back consiste à lire la piste de la carte lorsque la puce est défectueuse, ce qui revient à effectuer une transaction à l'ancienne avec tous les risques de fraude que ça comporte. Ce problème peut être causé par une mauvaise qualité des lecteurs de la puce ou à un disfonctionnement au niveau de la puce elle-même.

Au niveau des transactions avec les TPE, il arrive qu'au lieu de passer la carte dans le terminal, les commerçants utilisent les facturettes qui seront saisies plus tard au service monétique afin de débiter le client et créditer le commerçant. Les facturettes contiennent toutes les données sensibles de la carte et du porteur. Il peut avoir fraude, vol de données, pertes de données, mauvaises manipulations tout au long du circuit de traitement des facturettes. Le CSMM qui saisie les cartes les reçoit parfois avec du retard ou avec des informations incomplètes ou inexactes. Les principaux facteurs qui poussent les commerçants à utiliser les facturettes sont les problèmes techniques de certains TPE, des problèmes de réseaux, une méconnaissance des bonnes pratiques de la part des commerçants. Il faut aussi noter que le traitement des facturettes au sein même du CSMM pose problème. Un temps important est mis pour le traitement à cause d'une méconnaissance des risques encourus, d'un problème d'organisation et d'un manque de temps.

Pour les cartes, force est de constater que malgré les efforts fournis pour le déploiement des cartes à puce, toutes les cartes ne sont pas conformes à la norme EMV. Les cartes non-conformes sont pour toutes les filiales, hormis la SGBS, des cartes privatives qui ne peuvent être utilisées que dans le réseau des filiales elles mêmes ; ce qui limite ou annule même les risques de fraude. Mas avec l'arrivé de l'interbancarité sous régionale qui s'appliquera aussi aux cartes privatives des filiales qui sont dans l'espace UEMOA, le risque de fraude va augmenter. Seule la SGBS dispose d'une carte visa, qui marche à l'international et qui n'est pas à puce. Le risque est plus accru vu les caractéristique de cette carte car la carte en question fait partie du haut de gamme et est susceptible de faire des transactions avec de gros montants. Ce facteur peut entrainer des pertes considérables pour la filiale SGBS.

Tableau 8 : récapitulatif du niveau d'application des normes EMV par filiale

Filiale	Pays	Taux d'application de la norme EMV
BFV-SG	Madagascar	40%
SGB	Bénin	60%
SGBB	Burkina Fasso	67%
SGBC	Cameroun	60%
SGBCI	Cote d'ivoir	71%
SGBG	Guinée	50%
SGBGE	Guinée equatoriale	50%
SGBS	Senegal	58%
SGM	Mauritanie	40%
SGT	Tchad	50%

Source : CSMM (2010)

Nous notons donc que pour les commerçants n'utilisant pas les facturettes ne seront pas exposés au transfert de responsabilité pour les transactions frauduleuses. Par contre, les filiales sont exposées à une fraude massive si l'utilisation de la carte à puce n'est pas généralisée.

Nous avons aussi noté que bon nombre de GAB et TPE (et ça ne s'arête pas seulement au cas de la SOCIETE GENERALE mais ça touche toutes les banques) ne parviennent pas à générer correctement les nombres aléatoires requis par le protocole EMV pour authentifier de façon sûre les demandes de transaction. Ceci rend ces dispositifs de paiement vulnérables aux attaques qui permettent aux criminels d'envoyer des demandes de transactions frauduleuses. Ceci est un problème supplémentaire que le CSMM doit gérer pour ses filiales.

- La norme PCI

L'analyse de l'application de la norme PCI couvre un champ très large car en dehors de des outils utilisés pour les transactions et pour le traitement des transactions, le PCI DSS concerne la manière d'agir des collaborateurs dans leurs échanges d'informations.

Pour ce qui est des échanges d'informations entre les collaborateurs du CSMM eux même ou entre le CSMM et les filiales, les PAN ne sont pas toujours cryptés ou codé lors d'échange de mails. Un sondage que nous avons effectué au niveau de certains agents a permis de voir qu'environ 10% des mails échangés contiennent des informations non codé ou crypté concernant des PAN. Les informations peuvent être détournées par des personnes malveillantes avec tous les risques que ça comporte.

Sur les 12 conditions de la norme, notre étude permet d'affirmer que 7 sont appliquées, 4 sont appliquées partiellement et une n'est pas appliquée. Même si la majorité des conditions est respectée, le CSMM et les filiales qu'il gère ne sont pas encore conformes à la norme. La mise en conformité suit plusieurs étapes et la première de ces étapes n'est même pas encore franchie. Des réflexions et des travaux sont cependant lancés avec la SGBS comme filiale teste pour arriver à cette conformité avec la norme.

La non-conformité de tout le réseau aux normes PCI DSS fait courir au CSMM et à ses filiales les risques suivants :

- la sécurité globale du système fait défaut ;
- il n'y pas une mise en place en interne d'un dispositif adéquat pouvant assurer une meilleure sécurité des informations de cartes bancaires en particulier et du système d'information en général en terme de confidentialité, d'intégrité et de disponibilité ;
- rien ne nous assure qu'il n'y aura pas de fuite de données ou d'attaque du système.
- la non protection des données sensibles des porteurs que sont le PAN, le nom du porteur, la date d'expiration, le CVV, le PIN,
- les exigences réglementaires des réseaux internationaux pour les transactions ne sont pas respectées ce qui fait courir à la banque des risques de perte ou de sanction ;
- une vulnérabilité et le manque de protection pour lutter contre la fraude sans compter le risque encouru pour l'image de l'institution.

6.2 Recommandations

Nous avons pour cette partie suivi la logique de l'analyse ; De Ce fait, nous formulerons d'abord des recommandations part rapport à l'analyse des apports du CSMM sur la gestion de l'activité monétique des filiales et ensuite nous formulerons des recommandations pour une meilleure conformité aux normes EMV et PCI tout ceci dans un souci de sécurité et de fiabilité.

6.2.1 Recommandations portant sur l'organisation et la gestion de l'activité

En cherchant à harmoniser, à mutualiser, le CSMM se heurte à certaines barrières dues au fait que les pratiques ne sont pas harmonisées au niveau des filiales elles mêmes. Chaque filiale a sa propre organisation, sa propre manière de comptabiliser, ses propres besoin. Il y a aussi les barrières d'ordre réglementaires, légaux, fiscaux spécifiques à chaque pays. Tout ce que nous avons cité montre que cette mutualisation n'arrivera sans doute pas à se faire de sorte qu'on puisse dire qu'un jour tout est harmonisé à 100%. Un travail d'harmonisation, qui ne relève peut être pas du CSMM à 100% est à faire afin de faciliter le travail. Ce travail commence par un schéma comptable monétique commun que le CSMM doit mettre en place et le proposer au CSMCR qui se chargera de sa validation et de sa mise en place.

Il faut aussi noter que l'harmonisation a ses limites. Le fait de vouloir harmoniser ne doit pas mettre de côté les réalités de chaque filiale et de chaque pays. Donc il faudrait maîtriser la réalité de chaque pays, les prendre en compte harmoniser ce qui peut l'être et ne pas harmoniser le reste. Tout ceci dans le but d'une meilleur productivité et permettre aux filiales d'atteindre leur objectif.

Un manque de connaissance, d'organisation, de suivi est noté au niveau des filiales et ça entraine une diminution de l'efficacité du CSMM et un ralentissement dans le déroulement de certaines activités. Le CSMM n'a parfois pas de correspondant monétique de qualité dans les filiales. Des actions doivent être menées dans ce sens avec l'aide des directions des filiales car il en va de l'intérêt de tous.

Malgré les efforts qui sont fournis et les réorganisations qui se font au fil du temps en fonction des besoins, le CSMM devrait améliorer la manière dont les tâches sont réparties. Ceci permettra d'augmenter l'efficacité du centre et de limiter certains risques et disfonctionnement. Pour y arriver la première étape sera d'établir une grille de répartition des tâches au niveau de chaque poste et après d'analyser pour trouver les failles et apporter des améliorations.

Un autre aspect que nous aimerions souligner dans ce mémoire concerne le volet commercial au niveau des filiales. Le CSMM devrait voir, en fonction de ses attributions et de ses limites, comment booster et mobiliser les filiales concernant la commercialisation et la vulgarisation des produits et services monétiques. Nous remarquons lors du lancement de certains projets ou de produit que le degré d'adhésion est différent en fonction des filiales.

Toutes ces recommandations s'adressent à la direction du CSMM. Elle s'adresse à l'équipe dirigeante et à tous les chefs de pôle dans un sens plus large. C'est à la direction de faire un plan d'action et d'impliquer efficacement les différents acteurs.

6.2.2 Recommandations relative à l'application des normes

A- L'application de la norme EMV :

Pour une meilleure efficacité et une meilleure application de la norme EMV, le CSMM devrait :

- Configurer les TPE, les GAB et les cartes des filiales afin de rejeter toute transaction fall-back. Il est techniquement possible en donnant des instructions au processeur qui s'occupe du système d'information monétique de la filiale d'empêcher qu'il y ait des transactions en fall-back. Même si cette disposition n'arrangera parfois pas les commerçants qui peuvent perdre des clients, elle permettra de diminuer considérablement le risque de fraude. De plus le fait d'accepter les transactions fall-back est un risque de recevoir des chargebacks mais surtout de faire face au transfert de responsabilité. Nous rappelons que les transactions fall-back sont les transactions pendant lesquels la lecture de la puce n'a pas pu se faire. De ce fait, c'est la puce qui est lue, avec tous les risques que ça comporte.

- les commerçants doivent être sensibilisés sur l'utilisation des TPE et les actions à mener pour lutter contre les fraudeurs. Chaque filiale doit, avec l'aide du CSMM assurer un suivi, envoyer des technico-commerciaux pour la maintenance du parc TPE et aussi assister, conseiller et former les commerçants. Ces pratiques permettront aussi de diminuer l'utilisation des facturettes. Un deadline doit être fixé et un plan d'action mis en place pour éliminer progressivement les facturettes. En ce qui concerne toujours les facturettes, une nouvelle répartition des tâches doit être au sein du CSMM. Une personne spéciale doit être désignée pour la gestion des facturettes afin d'assurer un traitement rapide et un meilleur suivi.
- le déploiement des cartes EMV doit être finalisé afin que toutes les cartes soient maintenant EMV. L'urgence ce fait encore plus sentir du fait de l'arrivée de l'interbancarité sous régionale.

Normalement, pour pousser les différentes parties à engager les démarches pour tendre vers une totale conformité EMV les arguments ne manquent pas. Nous avons entre autre le transfert de responsabilité, les modifications à la législation ainsi que la volonté d'être perçue comme une entreprise responsable. Il faut donc une volonté de préserver les actifs informationnels de l'entité même ou des clients. En général, les organisations retardent la mise en place et l'application de moyens pour diminuer la fraude. Un travail de sensibilisation doit être effectué par les filiales sous l'impulsion du CSMM.

B- Le Respect à une conformité PCI DSS

Avant de pouvoir prétendre à une conformité PCI, il est préférable que certaines actions soient préalablement menées :

- les agents doivent d'abord être formés et sensibilisés, aussi bien au CSMM qu'au niveau des filiales, sur la sécurité des emails envoyés ;
- les agents doivent s'assurer que les PAN ou les données sur les porteurs soient toujours cryptés ou accompagnées de mot de passe ;
- les logiciels antivirus ou de détection peuvent être mis en place pour filtrer ou détruire tout mail entrant ou sortant qui comporte des informations sensibles non protégées ;

- les fichiers journaux doivent être sauvegardés et tenant lieu d'éléments de traçabilités pour des contrôles ultérieurs ;
- des caméras peuvent être mises en place au niveau des distributeurs pour assurer une prévision des risques de patrimoine sur les DAB ;
- le CSMM doit encourager les filiales à se doter de distributeurs qui disposent de caches au niveau du clavier numérique afin d'assurer une plus grande discrétion lors de l'entrée du mot de passe lorsque le commerçant effectue un retrait.

Les CSMM doit enfin piloter le projet de certification PCI de ses filiales. Pour cela les différentes étapes de mise en conformité doivent êtres suivies. Ces étapes sont :

- Compléter le rapport de conformité conformément aux instructions décrites ;
- s'assurer que les analyse des vulnérabilités ont été réalisées avec succès par un prestataire de services d'analyse agréé par le PCI SSC et se procurer auprès de ce dernier la preuve de l'exécution réussi de ces analyse ;
- compléter l'intégralité de l'attestation de conformité disponible sur le site internet du PCI SSC ;
- envoyer le rapport sur la conformité, la preuve de l'analyse réussie et l'attestation de conformité ainsi que toute autre documentation requise à la marque de carte de paiement ou à tout autre demandeur.

Pour arriver à une totale conformité, nous recommandons que les exigences suivantes soient suivies et implémentées par le CSMM et les filiales qu'il gère :

- la création et la gestion d'un réseau sécurisé. Même si nous avons constaté qu'un réseau sécurisé est existant dans toutes les institutions financières, celui-ci doit être renforcé au CSMM ;
- les données des titulaires de cartes doivent être protégées surtout à travers les facturettes et la systématisation de l'envoi d'informations cryptées ;
- la mise en place et la gestion d'un programme de vulnérabilité. Ce programme de vulnérabilité n'existe pas au CSMM.
- la mise en œuvre des mesure de contrôle d'accès strict ; nous n'avons pas pu effectuer les observations sur le contrôle d'accès au niveau des filiales mais en ce qui concerne le CSMM et la SGBS, le contrôle n'est pas strict et comporte plusieurs failles ;
- la surveillance et le test régulier des réseaux, les équipes informatiques ne devraient ainsi pas seulement se limiter à l'installation d'anti virus ;

- la gestion d'une politique de sécurité des informations : sur ce point, le CSMM ne devrait pas seulement se limiter aux mails groupés envoyés par le groupe SG mais développer et animer une politique spécifique.

De même, afin d'atteindre une conformité totale sur tout le périmètre PCI DSS des filiales, nous avons identifié différents chantiers sous la responsabilité du CSMM, du CSMSI et de la filiale concernée. La déclinaison de ces actions peut être établie dans une matrice de responsabilité appelée RACI et un plan d'action qui conduiront à un plan de remediation.

Du point de vue des clients et commerçants, nous recommandons de mettre en conformité en priorité la partie acquisition TPE et call center puis de mettre en conformité le système d'information de la filiale le plus tôt possible.

Différentes réunions devront être tenues par les parties prenantes et nous énumérons ci-dessous les différents sujets et ateliers à mettre en place pour avancer sur le projet :

- présentation du projet,
- utilisation et stockage des données monétiques,
- situation réseau et sécurité de la filiale,
- cadrage et PCI-DSS au CSMM avec la stratégie de déploiement de la mise en conformité des filiales CSMM,
- revue des procédures et pratiques des départements monétiques des filiales,
- PCI DSS et canaux d'acceptation TPE et GAB,
- procédures monétiques aux niveaux des agences des différentes filiales,
- revue du centre d'appel d'un point de vue PCI DSS,

Force est donc de constater qu'une conformité passe d'abord par un audit de tout le processus et des outils monétiques de la filiale.

6.2.3 Comment améliorer l'environnement du CSMM et la gestion des RH ?

Autant les ressources humaines constituent la force Du CSMM autant elles constituent son talon d'Achille. Un audit des ressources humaines doit être fait pour chercher les points à améliorer et mettre en place un plan d'action efficace.

Pour que l'environnement soit d'abord plus professionnel, la première règle devrait être l'instauration d'un « dress-code ». Les employés ne viennent parfois pas au travail avec une tenue correct et ça nuit à l'image d'excellence du centre.

Les contrats d'expatriations Afrique-Afrique sont décevants pour certains expatriés car les traitements ne sont pas les mêmes d'une personne à une autre. Une mise à niveau devrait se faire pour éviter que certains expatriés se sente moins lésés.

Nous recommandons aussi très fortement que le traitement des agents locaux soit revu. Une prime devrai être instaurée par rapport à la charge de travail supplémentaire et aux risque supporté. Les agents travaillent sous pression pour dix filiales, et aussi ils se sentent frustrés par rapport au traitement des expatriés.

Aussi, pour rendre les agents plus polyvalents et éviter la monotonie, il serait préférable que les agents du CSMM tournent d'un poste à un autre. Par exemple, celui qui fait la gestion des litiges au bout de deux ans change pour faire ajustement comptable, puis gestion des anomalies etc. Puisque le CSMM se veut être un centre d'expertise, les agents doivent d'abord être des experts. Et le meilleur moyen d'y arriver est d'adopter la démarche proposée ci-dessus.

Enfin, nous insistons sur le volet formation. Car il est important de former les agents du CSMM. La monétique est en perpétuelle évolution et il est primordial qu'un plan de formation soit mis en place pour chaque employé du CSMM.

Nous recommandons aussi l'instauration d'un vrai service ressource humaine pour la gestion des carrières des agents du CSMM et aussi la prise en charge de tous les aspects du côté sensible qu'est la gestion des ressources humaines.

6.2.4 Les innovations à apporter pour avoir une longueur d'avance sur la concurrence :

La première recommandation que nous faisons est l'instauration d'un système de surveillance permanente très efficace afin de s'assurer du respect des procédures et des engagements du CSMM.

Une comptabilité analytique doit être mise en place pour optimiser le coût de fonctionnement du CSMM. Ça permettra aux filiales de supporter une facture moins élevée. Ceci leur permettra aussi d'être plus rentables et baisser aussi les prix afin d'être plus attractifs par rapport à la concurrence.

La dernière recommandation que nous voudrions faire sur ce point est l'expansion du CSMM. Le CSMM devrait ne pas se limiter à l'Afrique subsaharienne et Madagascar. Il devrait couvrir d'autres filiales comme la SG Ghana, ou les filiales maghrébines.

La CSMM devrait mettre en place un réseau privatif pour toutes les filiales qu'elle prend en charge. Lorsqu'un porteur de carte SGBS effectue une transaction à la SGBCI, c'est considéré comme une transaction VISA internationale ou à la limite une transaction GIM. Certain grands groupes ont leur propre réseau. Ce réseau privatif permettra à la transaction citée plus haut d'être considérée comme une transaction locale donc non facturée au porteur de carte. C'est un impératif pour la satisfaction de la clientèle. Ça demande juste un développement à faire par le processeur et aussi la mise en place au CSMM d'un système de compensation efficace entre filiales.

Toujours dans le même ordre d'idée, les activités du CSMM ne devrait plus se limiter uniquement à la monétique (cartes, tpe, gab) mais le centre devrait s'ouvrir au e-banking en général et centraliser la gestion du e-banking des filiales SG. Ça permettra aux filiales de la SG de se mettre à niveau par rapport à la concurrence voir même dépasser la concurrence.
Le tableau ci-dessous récapitule les solutions e-banking faites par les banques de la place et non pris en charge par le CSMM. Nous recommandons que tous les produits non disponibles soient pris en charge et intégrés par le CSMM.

Tableau 9 : disponibilité des produits e-banking :

Produit	**Disponible ou Pas Disponible**
Carte	Disponible
Tpe	Disponible
Gab	Disponible
Instant PIN issue	Non disponible
Instant card issue	Non disponible

Banque en ligne	Non disponible
Cartes prépayées	Non disponible

Source : CSMM (2010)

6.2.5 Recommandations relatives à la gestion des risques

Nous avons constaté que CSMM ne dispose d'une cartographie des risques propres à la monétique, aussi doit –il :

- mettre en place une structure de prévention des risques ;
- recentrer les risques au niveau de chaque métier ;
- disposer d'une politique de sécurité pour la monétique ;
- disposer de tous les règlements de la BCEAO en matière de gestion des cartes bancaires ;
- faire appel périodiquement à des auditeurs externes pour évaluer les risques liés à la gestion du système monétique de CSMM.

Cette cartographie permettra de synthétiser les risques courus par le CSMM et les filiales dans le domaine de la monétique.
Les risques qui seront à fréquence élevée avec un impact important sont considérés comme non tolérables et des actions rapides et adéquates devront être mises en place.

Pour y arriver, voici les étapes que nous leur recommandons :

- recenser les principaux processus et les principales activités du CSMM ;
- analyser et faire sortir les principaux risques qui peuvent affecter ces processus ;
- évaluer le risque en déterminant la fréquence de survenance et l'impact en cas de survenance ;
- identifier et évaluer les solutions pour minimiser les risques ;
- enfin, le risque net doit être évalué ; c'est-à-dire le risque tel qu'il existe dans l'entreprise après la mise en place des moyens de contrôle.

Elaborer une cartographie des risques n'est pas une fin en soi mais permet de faire un état des lieux pour mettre en place des outils correctifs. Il permet de se poser les bonnes questions au bon moment. Il peut également être le déclencheur pour réaliser un plan de continuité de l'activité.

Le plan de continuité est en cours d'élaboration. Et peut faire l'objet de développement à part entière.

Un plan de continuité d'activité (PCA) est un document expliquant la procédure que l'entreprise doit élaborer et mettre en place en cas de survenance d'un risque qui l'empêcherait de pouvoir continuer son activité. Le mettre en place est entre autres un moyen de réduire les risques. Elle nécessite la nomination d'un chef de projet, une amélioration du système avec un cahier de charge puis des tests fréquents. C'est un document vivant qui douit être mis à jour régulièrement.

Conclusion chapitre 6

Nous pouvons retenir les recommandations prioritaires ci-après :

- le CSMM qui saisie les cartes les reçoit parfois avec du retard ou avec des informations incomplètes ou inexactes ;
- toutes les cartes de CSMM ne sont pas conformes à la norme EMV ;
- le CSMM n'a parfois pas de correspondant monétique de qualité dans les filiales ;
- les commerçants doivent être sensibilisés sur l'utilisation des TPE et les actions à mener pour lutter contre les fraudeurs ;
- des caméras peuvent être mises en place au niveau des distributeurs pour assurer une prévision des risques de patrimoine sur les DAB ;
- le CSMM doit mettre en place une structure de prévention des risques.

CONCLUSION DE LA DEUXIEME PARTIE

Dans cette deuxième partie, nous avons fait la présentation de ce centre d'expertise monétique qu'est la CSMM à travers son historique, son organisation, son but mais aussi ses différentes activités et sa manière de fonctionner.
L'analyse de son fonctionnement nous a permis de mettre à jour l'apport et les améliorations indéniables du CSMM sur l'organisation de l'activité monétique même si c'est un centre nouveau et que des améliorations sont à apporter.
Nous avons aussi pu nous faire une idée du niveau d'application des normes PCI et EMV. Ces normes sont devenues incontournables et nous avons apporté des recommandations qui permettront une meilleure conformité à ces normes et une diminution des risques

En somme, nous pouvons dire que le secteur de la monétique et de la monnaie électronique a des perspectives intéressantes dans l'UEMOA en général, et au Sénégal en particulier. En effet, l'importance que revêt ce secteur dans la dynamisation des échanges et le renforcement de la compétitivité au niveau sous régional et mondial nous commandait de nous y intéresser de plus prêt. Cependant le caractère quasi nouveau de ces nouveaux moyens de paiement méritait que l'on s'interroge sur les risques potentiels liés à leur utilisation, dans une otique de protection et de stabilisation de l'économie. Pour ce faire, nous avons analysé les risques d'utilisation de la monétique et de la monnaie électronique dans les systèmes de paiement au Sénégal, en nous fixant trois objectifs à l'intérieur desquels nous avons tiré les trois hypothèses suivantes :

- l'utilisation par les banques de la monétique et de la monnaie électronique peut être source de conflits entre les différents acteurs des transactions monétaires et financières au Sénégal ;
- l'utilisation par les banques de la monétique et de la monnaie électronique pose le problème de sécurisation des systèmes et moyens de paiement au Sénégal ;
- les risques de défaillance du réseau d'une banque dus à l'utilisation de la monétique et de la monnaie électronique ne peuvent pas affecter l'ensemble du système de paiement interbancaire au Sénégal.

L'analyse de ces hypothèses nous amène à conclure que les différents risques liés à l'utilisation de la monétique et de la monnaie électronique sont plus ou moins mis sous contrôle par la BCEAO et le GIM-UEMOA au Sénégal en particulier, et dans la sous région de l'UEMOA en général. En effet, les résultats de notre étude démontrent que ces risques interviennent à différents niveaux. D'abord au niveau juridique, ensuite au niveau de la sécurité des systèmes et moyens de paiement, et enfin au niveau de l'ensemble du système bancaire et financier du Sénégal et de la sous région.

Au demeurant l'étude des risques juridiques montre que la plupart sont issus des risques opérationnels relatifs à la fraude, à travers les tentatives d'intrusion dans le système, d'usurpation d'identité ou de blanchiment d'argent qui est un risque réel même si, le GIM n'a à ce jour enregistré aucun procès, ni procéder à l'arrestation d'un fraudeur. Le GIM a juste enregistré quelques tentatives d'intrusions issues d'une fraude importé, et quelques réclamations d'ordres opérationnelles de ses membres sur l'utilisation de la plate forme de paiement du GIM.

Par contre la sécurité des systèmes et moyens de paiement du GIM est fiable, en ce sens qu'il utilise les dernières technologies en la matière telles que la connexion par le réseau V-SAT, VPN ou l'utilisation de la norme EMV, pour la sécurité des cartes prépayées du GIM-UEMOA.

Par ailleurs, la gestion du risque systémique est assurée en amont par le GIM et en aval par la BCEAO. Ce qui garantie un double niveau de sécurité du système qui favorise la stabilité de l'ensemble du système bancaire et financier du Sénégal en particulier et de l'UEMOA en général. Cela nous amène à confirmer nos deux premières hypothèses et à infirmer la dernière. Toutefois, l'insuffisance de la maîtrise du système monétique et de la monnaie électronique, l'insuffisance de membres connectés au réseau GIM liés aux travaux y relatifs et l'absence d'outils de gestion fiable des risques de fraude internes, nous a amené à émettre les quelques recommandations suivantes : renforcer les capacités de gestion des différents acteurs de la monétique et de la monnaie électronique ; vulgariser et négocier davantage le service délégataire, et l'accélération de la mise en place de la norme PCI-DSS pour une meilleur gestion des risques de fraudes aussi bien internes qu'externes.

Après avoir procéder à l'analyse des résultats, nous avons surtout constaté des insuffisances au plan technique et de la formation de CSMM. En effet, il nous proposons quelques recommandations susceptibles d'améliorer le fonctionnement de la monétique au Sénégal en particulier, et dans l'UEMOA en général :

- Renforcer les capacités de gestion des acteurs : Un bon renforcement de capacité pourrait améliorer la gestion des activités monétiques et de la monnaie électronique dans l'UEMOA. En effet, une meilleure maîtrise des processus d'utilisation de la monétique, et des mécanismes d'alertes sur la gestion du risque permettra de réduire le nombre de réclamation des membres du GIM, mais aussi de réduire les différents risques liés à son utilisation.

- Accélérer le processus de mise en place d'une cartographie des risques : Etant en projet et en cours d'élaboration, il s'agira d'accélérer sa mise en place afin d'avoir rapidement une meilleure visibilité sur les risques opérationnels et de mettre en place des points de contrôles fiables.

- Vulgariser le service délégataire auprès des membres : Le service délégataire est celui qui permet au GIM d'effectuer pour le compte de ses membres des travaux leur permettant de se connecter au réseau GIM en l'espace de 3 mois. Or certains membre prennent en charge eux -même leur travaux de connexion au réseau GIM et cela peut aller jusqu'à 3 ans avant que cela ne soit effectif. Ainsi la vulgarisation de ce service, avec un renforcement de la capacité de négociation permettra d'accroitre le nombre de membres connectés afin de dynamiser davantage les transactions monétiques.

- Booster la mise en place de la norme PCI-DSS chez tous les acteurs : La mise en place rapide de cette norme permettra de mieux gérer les tentatives de fraude aussi bien au niveau interne qu'externe des entreprises bénéficiaires des instruments de la monétique tenus par GIM-UEMOA.

- Consolider la position du Sénégal en matière monétique et de monnaie électronique : Dans la sous région de l'UEMOA, le Sénégal est l'un des pays qui a une certaine visibilité au niveau démocratique et de la stabilité. Cela implique qu'il représente un des pays où le risque pays est faible contrairement à ses concurrents directs tels que la

Côte d' Ivoire, le Niger ou le Mali. Ainsi la consolidation de ce pays dans sa position de leader permettra de garantir quelque peu la pérennité des installations GIM, au regard du fait également que le siège se trouve à Dakar.

CONCLUSION GENERALE

La BHFM qui s'occupe de l'activité banque de détail à l'internationale du groupe Société Générale cherche avant tout à normaliser ses activités, à les mutualiser, à développer des synergies, à maîtriser les risques opérationnels et renforcer la qualité du service clients. Cette démarche est passée par le regroupement de la fonction support monétique de ses filiales d'Afrique subsaharienne au sein du Centre des Services Mutualisés Monétique.
La création de ce centre regroupe des défis techniques, organisationnels, humains qui sont entrain d'être relevés petit à petit.

Pour le groupe Société Générale, l'intérêt de ce centre peut se résumer en ces quelques points : moins de risques, moins de coûts, plus d'innovation, plus de sécurité, plus de rapidité. Les filiales, clientes du CSMM, sont unanimes pour donner une appréciation positive du centre grâce au service de grande qualité rendu. Cet intérêt est d'autant plus partagé que le centre a atteint pleinement les objectifs qui lui ont été fixés et ceci avec efficience malgré les limites que le centre essaie de surmonter. Même si les objectifs ont évolué depuis sa création, le maître mot reste la création. Ce modèle a aussi montré sont efficacité en permettant à la Société Générale de rouvrir rapidement ses portes après la crise ivoirienne.

Un accent particulier doit être mis sur la connaissance et l'application des normes si le CSMM veut un jour remplir pleinement son rôle et apporter une vraie plus-value. Le non respect des normes expose le CSMM et les filiales qu'il gère à des risques opérationnels majeurs qui sont un frein pour le bon fonctionnement des filiales. L'application des normes aura pour conséquence le fait que les transactions seront plus sécurisées, les porteurs plus confiants, plus à l'aise et une hausse du taux de bancarisation par la suite ; d'où la nécessité de mettre l'accent sur les normes.

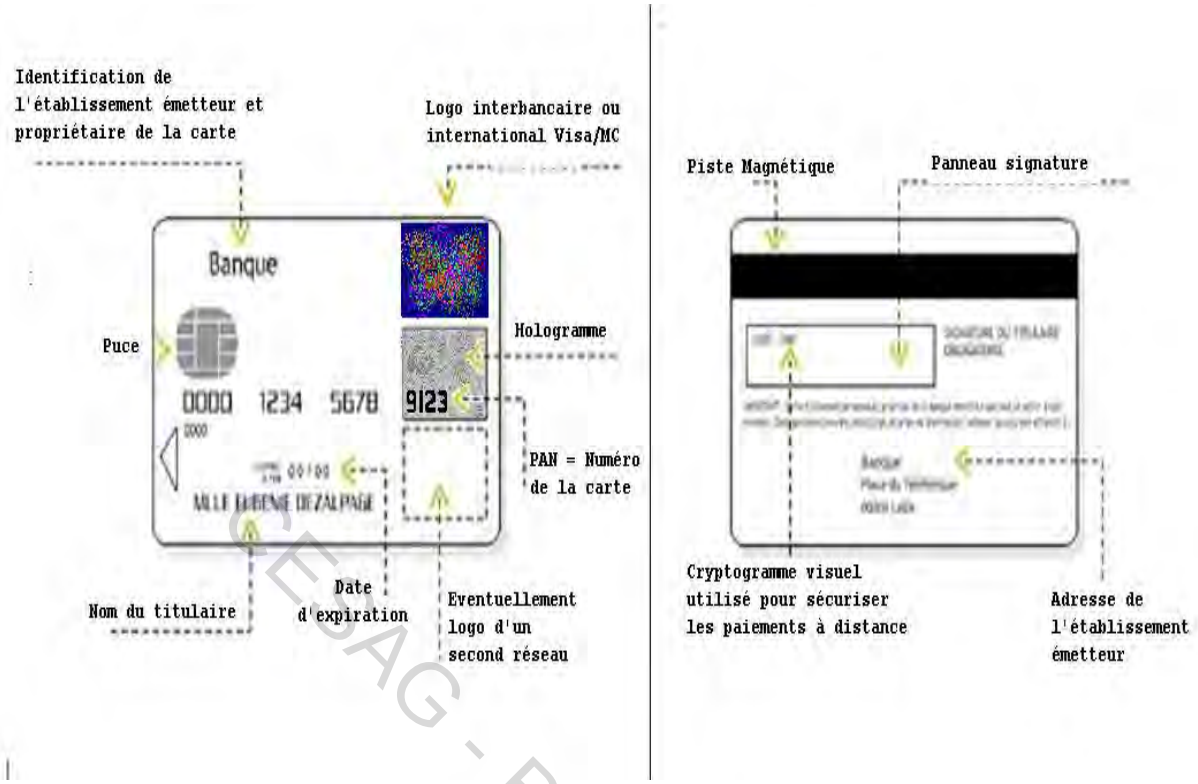
Dans un cadre plus général, ce centre participe au développement de la monétique en Afrique parce qu'il aide à la réalisation de l'enjeu majeur qui consiste pour les banques, à bâtir et proposer une offre monétique compétitive aux populations africaines de plus en plus exigeantes. Cela passera nécessairement par une maîtrise des coûts d'investissement et d'exploitation qui sont relativement élevés.

Cette étude nous a permis de nous familiariser à la notion de mutualisation des services, de monétique et de ses normes afin de mieux cerner, de mieux appréhender le fonctionnement du

CSMM. Cependant, vu que c'est une entité assez spécifique avec des règles de gestion qui diffèrent des sociétés « classiques », nous nous demandons si les outils et méthodes de contrôle, les outils d'aide à la prise de décision, les outils et modèles de contrôle de gestion mis en place généralement dans les entreprises peuvent s'adapter au CSMM. Si oui, comment ? Ces questions peuvent faire l'objet d'une étude ultérieure.

ANNEXES

ANNEXE 1 : LA CARTE BANCAIRE



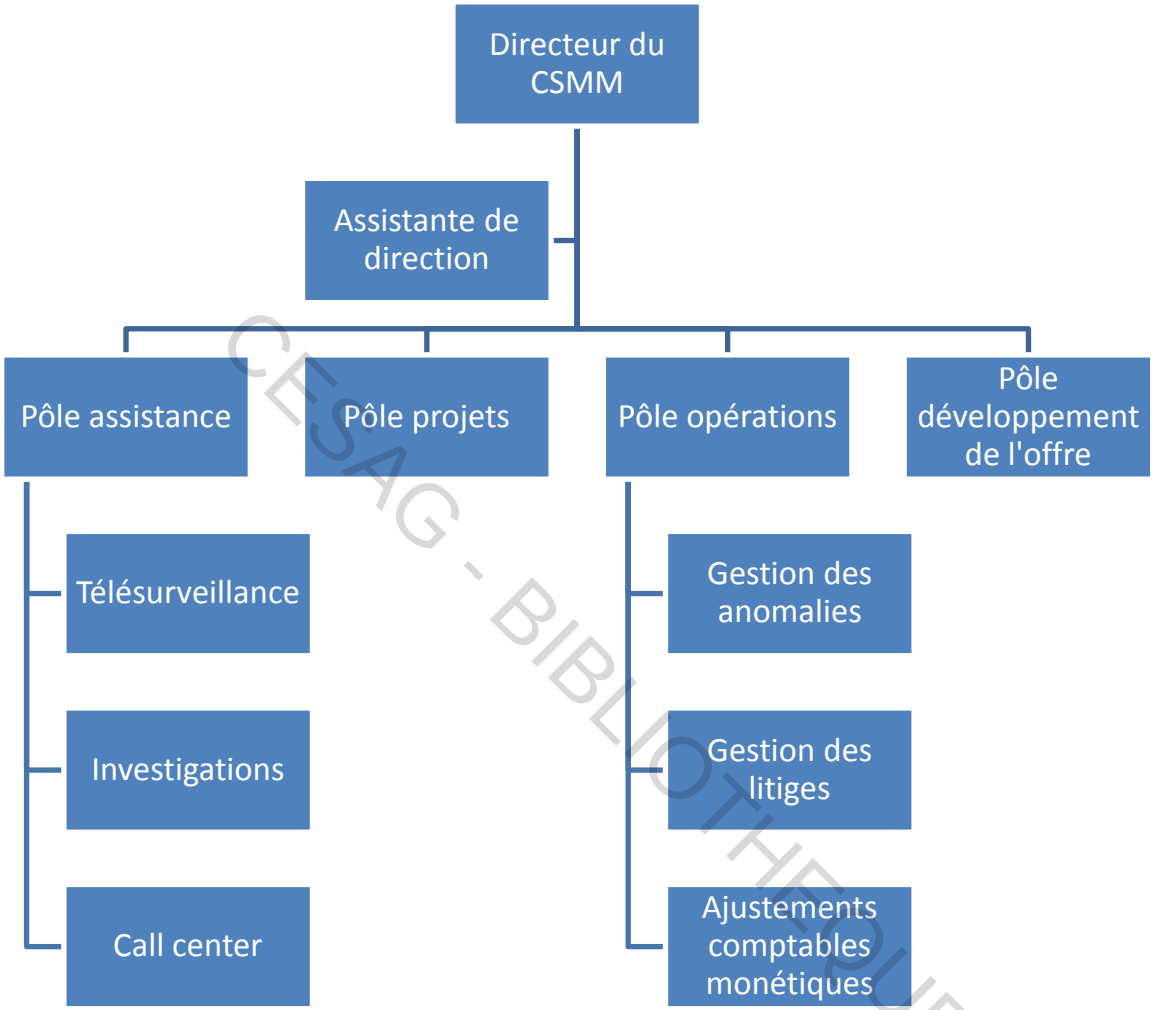
Source : Document interne du CSMM

Annexe 2 : Guide d'entretien

1.) Connaissance générale du CSMM
Quel est le statu juridique du CSMM
De qui dépend t-il ?
Objectif du CSMM
Qui finance les activités du CSMM ?
2.) Les activités du CSMM projets gérés par le CSMM
Comment se fait le transfert d'activités ?
Comment se décide le lancement d'un nouveau projet ?
Explication sommaire des activités des différents pôles
3.) Le bilan et l'avenir du CSMM
Comment se fait la mesure de la performance ?
Que disent les filiales sur le CSMM ?
Prochaine étape après le CSMM ? Vision de l'avenir ?
4.) La monétique en général
Intérêt de la monétique pour l'Afrique
Les normes en monétique

Source : Nous même

Annexe 3 : Organigramme du CSMM



Source : entretiens.

Annexe 4 : Questionnaire sur l'application de la norme PCI DSS

QUESTIONS	OUI	NON
Avez-vous une bonne connaissance des normes PCI ?		
Les utilisateurs ont-ils chacun leur ID ?		
Les anti-virus sont ils à jour ?		
Les pare feu sont ils activés ?		
Les pare feu et routeurs sont ils configurés conformément aux normes PCI ?		
Existe-t-il un accès direct aux données sensibles depuis internet ?		
Les mots de passe par défaut sont ils changés systématiquement ?		
L'entreprise a-t-elle une politique de sécurité satisfaisante ?		
Cette politique est elle bien appliquée ?		
Les données échangées sont elles cryptées ?		
Existe-t-il des applications, sur la protection des données, propres à l'entreprise ?		
Les codes secrets et les cartes sont ils stockés dans un endroit sécurisé avec accès restreint ?		

Sources : Revue de littérature

BIBLIOGRAPHIE

1. AVANEL Yvon (2007), Les cartes bancaires condamnées à l'innovation, *Revue Banque* (688) : 74-77.
2. BALKENHOL Bernd (1990), *Banques et petites entreprises en Afrique de l'Ouest : Problèmes et possibilités liés à leur rapprochement*, L'Harmattan, Paris, 191 pages.
3. BOUTILLIER Sophie, GOGUEL D'ALLONDANS Alban, UZUNIDIS Dimitri, LABERE Nelly (2005), *Méthodologie de la thèse et du mémoire*, Studyrama, France, 239 pages.
4. CARPENTIER Jean-François (2009), *La sécurité informatique dans la petite entreprise - Etat de l'art et Bonnes Pratiques*, Editions ENI, Paris, 278 pages.
5. CIFPB (1991), *La recherche d'une meilleure productivité pour les banques africaines*, L'Harmattan, Paris, 196 pages.
6. COULIBALY Sayon (2010), *Critères de distinction entre les effets de commerce*, http://univ-jurisocial.over-blog.com/article-criteres-de-distinction-entre-les-effets-de-commerce-60723173.html
7. DABO Bacary (2005), *Réforme des systèmes monétiques dans l'UEMOA*, Sud Quotidien, (1342) : 6 .
8. DUJARDIN Brigitte (2006), *Mutualiser pour répondre à de nouveaux besoins*, http://bbf.enssib.fr/consulter/bbf-2006-05-0101-010
9. DANCETTE Jeanne, WEGNEZ Léon, RETHORE Christophe (2000), *Dictionnaire analytique de la distribution*, Edition PUM, Montréal, 347 pages.
10. De COUSSERGUES Sylvie (2008), *Gestion de la banque*, 5ème édition, Dunod, Paris, 272 pages.
11. DJELLAL Faridah, GALLOUJ Faïz (2002), *Nouvelle économie des services et innovation*, L'Harmattan, Paris, 307 pages.
12. DRAGON Claude, GEIBEN Didier, NALLARD Gilbert (2002), *La carte et ses atouts*, Revue Banque, Paris, 126 pages.
13. DUPERON Olivier (2011), *Les services publics locaux et la concurrence : Entre intérêt général et marché*, L'Harmattan, Paris, 206 pages.
14. GUIDERE Mathieu (2004), *Méthodologie de recherche*, Ellipses, Paris, 127 pages.
15. FAY Aymé (1997), *Dico, Banque, Monétique, Euro*, La maison du dictionnaire, Paris, 203 pages
16. HALLEPEE Didier (2010), *L'univers de la monétique : Historique, fonctionnement et perspectives*, Carrefour du net, Paris, 170 pages

17. HOUNYONOU Lucien (2006), Pourquoi utiliser les cartes, *Le magazine de l'entreprise*, (51) : 50.
18. JOLY Cathie-Rosalie (2008), Le paiement mobile en question, *Mobiles magazine*, (119) : 22
19. MASOUNAVE Annick (2007), La banque de détail dans les pays émergents, *Revue banque*, (688) : 24-37.
20. MARTORY Bernard, DELAY Christine, SIGUIER Fabien (2008), *Piloter les performances RH: La création de valeur par les ressources humaines*, Editions Liaisons, France, 193 pages
21. MOSTAFA Hashem Shérif (2007), *Paiements électroniques sécurisés, PPUR*, Lausanne, 582 pages.
22. MOSTAFA Hashem Shérif, AHMED Serhrouchni, (2000), *Paiements électroniques sécurisés*, Eyrolles, Paris, 513 pages.
23. MOUCHTOURIS Antigone (2012), *L'observation : un outil de connaissance du monde*, L'harmattan, Paris, 172 pages.
24. NSABIMANA André (2002), *Organisation, régulation et efficacité économique du système d'intermédiation financière en Afrique*, Presses universitaires de Louvain, Belgique, 343 pages.
25. Les-HEBERT Michelle, GOYETTE Gabriel, BOUTIN Gérald (1997), *La recherche qualitative : Fondements et pratiques*, Editions Nouvelles AMS, Montréal, 117 pages.
26. ORDONNEAU Pascal (2011), *La bancarisation*, http://lecercle.lesechos.fr/cercle/abecedaire/b/221141386/bancarisation
27. Otman Gabriel (1998), *Les mots de la cyberculture*, Berlin, Paris, 474 pages.
28. PEREIRE Isaac (1865), *Principe de la constitution des banques et de l'organisation du crédit*, Dupont, Paris, 324 pages.
29. PIEDELIEVRE Stéphane (2007), *Instrument de crédit et de paiement*, Dalloz, Paris, 353 pages.
30. SOW Ousseynou (2002), *Directive N° 08/2002/CM UEMOA portant sur les mesures de promotion de la bancarisation et de l'utilisation des moyens de paiement scripturaux dans les états membres de L'UEMOA*, Ciga éditions, Dakar, 18 pages.
31. SOW Ousseynou (2002), *Union Economique et Monétaire Ouest Africaine (UEMOA) : règlement 15/2002/CM/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'UEMOA*, Ciga éditions, Dakar, 211 pages.

32. THUNIS Xavier (1996), *Responsabilité du banquier et automatisation des paiements*, Presses universitaires de Namur, Belgique, 362 pages.
33. TOURE Mounir M. (2007), *Introduction à la méthodologie de la recherche*, L'Harmattan, Paris, 214 pages.
34. VIDAL Philippe, LERENARD Jocelyn (2006), Une activité plus difficile à rentabiliser qu'il ne paraît, *Revue banque*, (677) : 26-29.