BANQUE CENTRALE DU CONGO

LE GOUVERNEUR

INSTRUCTION N° 42 RELATIVE AUX REGLES APPLICABLES A LA MONETIQUE EN REPUBLIQUE DEMOCRATIQUE DU CONGO

La Banque Centrale du Congo,

Vu la Loi organique n° 18/027 du 13 décembre 2018 portant organisation et fonctionnement de la Banque Centrale du Congo, spécialement en ses articles 10 et 71 ;

Vu la Loi n° 003/2002 du 02 février 2002 relative à l'activité et au contrôle des Etablissements de crédit, spécialement en son article 36 ;

Vu la Loi n°18/019 du 09 juillet 2018 relative aux systèmes de paiement et de règlement-titres ;

Considérant le besoin d'assurer l'interopérabilité des infrastructures monétiques en République Démocratique Congo ;

Considérant la nécessité de normaliser la carte de paiement et les canaux d'acquisition des opérations monétiques au niveau national ;

Edicte les dispositions suivantes :

TITRE Ier : DISPOSITIONS GENERALES

CHAPITRE Ier : DEFINITIONS

Article 1er : Définitions

Au sens de la présente Instruction, les mots, sigles et expressions ci-dessous, indifféremment employés au singulier ou au pluriel, s'entendent de la manière suivante :

1) **acceptation web** : processus de réception des paiements via un canal web ;
2) **accepteur :** partie ayant passé un accord avec un acquéreur pour accepter les transactions électroniques en contrepartie d'un bien ou d'un service rendu ;
3) **acquéreur :** institution financière qui met à la disposition de l'accepteur des canaux d'acquisition permettant d'effectuer des transactions par carte de paiement ou par tout autre procédé de transfert électronique de fonds ;

4) **agrégateur** : personne morale, prestataire de service technique de paiement qui offre des services de paiements et des solutions aux institutions financières dans le cadre des systèmes de paiement ;
5) **ATS (Automated Transfert System) :** Système de Transfert Automatisé opéré par la Banque Centrale ;
6) **Banque Centrale :** Banque Centrale du Congo ;
7) **BIN (Bank Identification Number) :** numéro d'identification de l'Emetteur de la carte de paiement ;
8) **carte virtuelle** : jeton logiciel généré de manière aléatoire par un émetteur, utilisé pour le paiement ;
9) **CENAREF :** Cellule Nationale des Renseignements Financiers ;
10) **DAB :** Distributeur Automatique des Billets ;
11) **Emetteur :** établissement financier qui fournit aux porteurs des instruments de paiement électronique afin d'effectuer des paiements et d'autres services associés ;
12) **EMV (Europay, Master Card and Visa)** : norme de sécurité des cartes de paiement à puce permettant notamment d'assurer l'interopérabilité quel que soit l'émetteur et quel que soit le GAB, le DAB, le TPE ou autres systèmes ;
13) **GAB :** Guichet Automatique de Banque ;
14) **interopérabilité :** situation dans laquelle des instruments de paiement relevant d'un système donné peuvent être utilisés dans un autre système ;
15) **incident :** évènement susceptible d'entrainer partiellement ou totalement l'interruption ou des perturbations des opérations dans un système monétique pour une durée supérieure à deux heures.
16) **instrument de paiement :** tout moyen, quel que soit le support utilisé, permettant à toute personne de transférer des fonds.
17) **monétique :** ensemble de traitements électroniques, informatiques et télématique nécessaires à la gestion de la carte de paiement ou de tout autre procédé de transfert électronique de fonds ;
18) **opérateur :** institution responsable du fonctionnement ou de l'administration d'un système.
19) **opération monétique :** opération par carte de paiement ou tout autre procédé de transfert électronique de fonds effectuée par des entités agréées ou autorisées ;

20) **PA-DSS (Payment Application Data Security Standard) :** norme de sécurité des données des applications de paiement ;

21) **Participant :** institution qui est partie à un accord établissant un système monétique et qui est chargée d'exécuter les obligations financières à sa charge résultant des ordres de paiement émis dans ce système ;

22) **PCI DSS (Payment Card Industry Data Security Standard) :** norme de sécurité des données de l'industrie des cartes de paiement, développée par les principales associations de cartes internationales ;

23) **PCI-PED (Payment Card Industry PIN Entry Device) :** norme de l'industrie des cartes de paiement permettant de sécuriser le traitement des opérations monétiques au niveau du dispositif d'acceptation du PIN ;

24) **PCI P2PE (Payment Card Industry Point-to-Point Encryption) :** norme de cryptage de l'industrie des cartes de paiement ;

25) **PIN (Personal Identification Number) :** code numérique permettant de vérifier l'identité du titulaire d'une carte ;

26) **porteur :** personne qui, en vertu d'un contrat conclu avec un émetteur, utilise une carte de paiement ou tout autre procédé de transfert électronique de fonds ;

27) **prestataire des services connexes ou critiques :** entité qui fournit, sur une base continue, des activités essentielles pour les opérations d'un système monétique.

28) **service d'acceptation Web :** service permettant le transfert de valeur monétaire par le site Web d'un fournisseur de biens ou d'un prestataire de services ;

29) **système monétique:** système régi par des procédures formelles standardisées et des règles communes pour le traitement et la compensation des opérations monétiques ;

30) **SLA (Service Level Agreement) :** accord sur le niveau de service conclu avec un fournisseur de service ayant pour objet le maintien d'un niveau de qualité des prestations ;

31) **Triple-DES / RSA :** algorithme de chiffrement des données pour toutes les données transmises et authentifiées entre chaque partie ;

32) **TPE :** Terminal de Paiement Electronique.

CHAPITRE II : OBJET ET CHAMP D'APPLICATION

Article 2 : Objet

La présente instruction a pour objet de fixer :

- les exigences devant être respectées par les personnes morales habilitées à mettre en place et/ou opérer un système monétique ;
- les obligations à respecter par les prestataires des services connexes aux systèmes monétiques ;
- les conditions et modalités de compensation et de règlement des opérations monétiques ;
- les règles qui sous-tendent l'interopérabilité des systèmes monétiques ;
- les normes applicables aux GAB, DAB et TPE ainsi qu'à la carte de paiement et à tout autre procédé de transfert électronique de fonds.

Article 3 : Champ d'application

La présente Instruction s'applique aux :

- opérateurs;
- participants ;
- émetteurs, accepteurs, acquéreurs et porteurs des cartes de paiement ou de tout autre procédé de transfert électronique de fonds ;
- prestataires des services connexes aux systèmes monétiques.

TITRE II : PARTICIPATION A UN SYSTEME MONETIQUE

CHAPITRE I^{er} : PARTICIPANTS, PRINCIPES ET FORMALISATION DE PARTICIPATION AU SYSTEME

Article 4 : Participants

Peuvent participer à un système monétique :

- la Banque Centrale ;
- le Trésor public ;
- les établissements de crédit ;
- les institutions de microfinance;
- les établissements de monnaie électronique ;
- les agents de règlement ;
- les services financiers de la poste ;
- les autres émetteurs agréés des instruments de paiements.

Article 5 : Principes de participation

L'opérateur prévoit, pour l'accès à ses services, des critères d'accès équitables et transparents, fondés sur une analyse des risques auxquels les participants l'exposent.

Les conditions de participation au système sont clairement énoncées, rendues publiques et justifiées en termes de sécurité et d'efficience de ce système.

A cet égard, l'opérateur dispose des procédures formelles et clairement définies pour l'adhésion, la suspension ou l'exclusion d'un participant qui enfreint les conditions susvisées ou qui n'y satisfait plus.

Article 6 : Formalisation de la participation au système

L'opérateur fixe les règles du système qu'il opère reprenant notamment :

- les conditions de participation, de suspension et d'exclusion du système ;
- les droits et les obligations de l'opérateur et des participants ainsi que des porteurs ;
- les règles et procédures d'exploitation du système ;
- les opérations de règlement effectuées par le biais du système ;
- le moment à partir duquel une opération revêt un caractère irrévocable et définitif ;
- les règles de compensation ;
- les risques liés à la participation au système ;
- les garanties constituées pour couvrir les obligations découlant de la participation au système.

Le requérant désirant participer audit système signe un acte d'adhésion.

CHAPITRE II: AGREMENT ET AUTORISATION

Article 7 : Dispositions générales

Conformément aux dispositions qui suivent, la Banque Centrale agrée ou autorise :

- les opérateurs, leurs dirigeants et leurs commissaires aux comptes ;
- les prestataires de services connexes, leurs dirigeants et leurs commissaires aux comptes ;
- les nouveaux instruments de paiement.

La demande d'agrément ou d'autorisation, en langue française, est introduite à la Banque Centrale/Direction ayant la surveillance des systèmes de paiement dans ses attributions.

La Banque Centrale rend sa décision dans un délai de soixante jours à compter de la réception du dossier complet. Pour les nouveaux instruments de paiement émis par les émetteurs régis par la loi bancaire, la Banque Centrale rend sa décision dans le délai d'un mois.

Dans l'examen du dossier, si la Banque Centrale estime nécessaire un complément d'informations ou une consultation d'une autorité de régulation étrangère, elle peut proroger le délai de traitement de la demande d'agrément. Dans ce cas, elle informe le requérant du nouveau délai de traitement.

Article 8 : Agrément de l'opérateur

L'exploitation ou la mise en service d'un système monétique en République Démocratique du Congo est conditionnée par l'obtention préalable de l'agrément de la Banque Centrale.

Le dossier d'agrément doit contenir, en trois (3) exemplaires, les documents ci-après en langue française :

- les statuts de l'établissement ;
- le document établissant les qualités et les pouvoirs des représentants légaux et/ou statutaires ;
- les renseignements sur les dirigeants de l'établissement ;
- l'identité des personnes détenant directement ou indirectement des participations dans le capital et la taille de leur participation ;
- les états financiers certifiés par un commissaire aux comptes agréé pour les établissements ayant plus d'une année de vie sociale ou le cas échéant, les états financiers prévisionnels ;

- le plan d'affaires ;
- les règles de fonctionnement du système monétique ;
- les spécifications techniques du système monétique ;
- l'architecture technique ;
- le coût des transactions et le mode de tarification ;
- les dispositifs de protection des utilisateurs ;
- le dispositif de contrôle interne mis en place ;
- les procédures de règlement applicables en situation ordinaire et de crise ;
- les procédures de gestion des risques.

Toute modification d'un des éléments susmentionnés nécessite l'accord préalable de la Banque Centrale.

La Banque Centrale peut, en tant que de besoin, réclamer toute information complémentaire qu'elle juge nécessaire pour le traitement de la demande d'agrément.

Lorsque le requérant est un Etablissement de crédit opérant en République Démocratique du Congo, il est, sous réserve d'une exigence expresse de la Banque Centrale, dispensé de la communication des documents repris aux cinq premiers tirets.

La gestion courante de l'opérateur doit être confiée à au moins deux personnes physiques justifiant d'une bonne moralité ou réputation et des aptitudes professionnelles requises pour l'exercice de leurs fonctions.

Le requérant est tenu de soumettre à la Banque Centrale un dossier de demande d'agrément en faveur de tous les membres de l'organe exécutif, des commissaires aux comptes et le cas échéant, de l'organe délibérant comprenant notamment les éléments suivants en langue française :

- le curriculum vitae ;
- l'extrait du casier judiciaire datant de moins de trois mois et pour les personnes ayant résidé à l'étranger au cours de trois dernières années précédant la demande d'agrément, un document équivalent dûment légalisé, délivré par le pays d'accueil ;
- l'attestation de résidence ;
- l'attestation de bonne vie et mœurs ;
- les copies des procès-verbaux notariés des réunions des organes délibérants et exécutifs ayant statué sur les désignations ;
- le document de l'autorité de surveillance des systèmes de paiement du pays d'origine ou de résidence, pour les personnes étrangères, attestant la conformité aux conditions d'agrément dans ledit pays ;

- la déclaration sur l'honneur sur la véracité des informations signées par les intéressés ;
- la rémunération et les autres avantages liés à la fonction ;
- les éléments justifiant la capacité à exercer les fonctions pour lesquels l'agrément est sollicité ;
- la preuve que le commissaire aux comptes est agréé à l'Ordre National des Experts Comptables.

Sous réserve d'une demande expresse de la Banque Centrale, le requérant est exempté de communiquer les documents repris à l'alinéa précédent pour les personnes ayant déjà été agréée.

Article 9 : Autorisation des prestataires des services connexes

Les prestataires des services connexes désirant s'établir en République Démocratique du Congo doivent obtenir une autorisation de la Banque Centrale.

Les prestataires des services connexes sont notamment:

- les agrégateurs ;
- les fabricants de plastique ;
- les centres de personnalisation des cartes ;
- les fournisseurs des canaux d'acquisition ;
- les éditeurs des logiciels et solutions monétiques ;
- les gestionnaires des plateformes de e-commerce.

Pour l'obtention de l'autorisation visée à l'alinéa 1er, les prestataires des services connexes doivent communiquer à la Banque Centrale, en langue française, les documents ci-après:

- les statuts de l'établissement ;
- le document établissant les qualités et les pouvoirs des représentants légaux et/ou statutaires ;
- les renseignements sur les principaux actionnaires et dirigeants de l'institution ;
- les identités des personnes détenant directement ou indirectement des participations dans le capital et la taille de leur participation ;
- la preuve de la bonne moralité des dirigeants ;
- les états financiers certifiés par un commissaire aux comptes agréé pour les établissements ayant plus d'une année de vie sociale ou le cas échéant, les états financiers prévisionnels ;
- le plan d'affaires ;
- les certificats techniques obtenus pour l'activité ;
- l'accord-type sur le niveau de service (SLA) ;

- les spécifications techniques et fonctionnelles des produits et services à offrir ;
- les procédures de règlement applicables en situation ordinaire et de crise ;
- les procédures de gestion des risques.

Lorsque l'opérateur d'un système monétique recours à un prestataire de service connexe étranger, il doit communiquer à la Banque Centrale, avant la signature du contrat, les documents ci-après sur le prestataire :

- l'autorisation ou l'agrément de l'autorité de regulation étrangère;
- les certificats techniques obtenus ;
- le projet de partenariat avec l'opérateur;
- l'engagement du prestataire étranger sur un niveau de qualité attendu et prédéterminé des prestations, répondant à un fonctionnement normal du service et, en cas d'incident, conduisant à l'activation de ses mécanismes de secours prévus par son plan de continuité ;
- l'engagement du prestataire étranger à se conformer aux procédures de l'opérateur concernant le contrôle du service fourni ;
- l'engagement du prestataire étranger à rendre compte à l'opérateur de façon régulière à l'opérateur de la manière dont est exercée l'activité externalisée.

Préalablement à la conclusion d'un contrat avec un prestataire de services connexes local, l'opérateur doit s'assurer que ledit prestataire a dument obtenu l'autorisation de la Banque Centrale pour les services offerts. Le manquement à cette obligation est passible d'une des sanctions prévues à l'article 46 de la présente instruction.

Article 10 : Autorisation pour l'émission de nouveaux instruments de paiement

Les émetteurs de nouveaux instruments de paiement doivent communiquer à la Banque Centrale :

- les spécifications techniques et fonctionnelles des instruments de paiement concernés ;
- la cartographie des risques liés au fonctionnement des instruments de paiement concernés ou un document d'identification de ces risques et les dispositifs mis en place pour leur gestion ;
- une description des mesures prises pour protéger les fonds des utilisateurs ;
- une description des mécanismes de contrôle interne mis en place dans le cadre des diligences en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme pour les produits à lancer ;
- le plan de continuité d'activités en cas de crise ou dysfonctionnement grave des infrastructures devant garantir le fonctionnement des produits à lancer.

CHAPITRE III : INTEROPERABILITE

Article 11 : Obligation d'interopérabilité

Tout système ou toute plateforme de paiement monétique, par carte, portemonnaie électronique ou tout autre instrument de paiement électronique, installé ou mis en œuvre en République Démocratique du Congo, ouvert au public, doit pouvoir échanger les données relatives aux transactions de paiement effectuées sur son réseau ou sur ceux des autres, avec tous les autres systèmes ou plateformes de paiement de même nature opérant en République Démocratique du Congo.

Ces mesures comprennent la mise en œuvre notamment des normes et règles communes, des systèmes d'échange des données des transactions, des liaisons des infrastructures de télécommunications ainsi que des fonctionnalités de routage des autorisations et de compensation des transactions en monnaie locale ou en devises étrangères ayant cours légal en République Démocratique du Congo.

Article 12 : Services interopérables

L'interopérabilité des systèmes monétiques doit notamment permettre au porteur:

- d'une carte de paiement d'effectuer des opérations de retrait de fonds sur tous les GAB et DAB ;
- d'une carte de paiement d'effectuer des opérations de versement de fonds sur tous les GAB;
- d'une carte de paiement d'effectuer des opérations de paiement des biens et services auprès d'un accepteur ;
- de monnaie électronique d'effectuer des opérations de paiement des biens et services auprès d'un accepteur ;
- de monnaie électronique d'effectuer des opérations de chargement et retrait de fonds auprès de tout agent, distributeur et émetteur de la monnaie électronique ainsi que sur tout DAB et GAB.

TITRE III : REGLES DU SYSTEME MONETIQUE

CHAPITRE I^{er}: REGLEMENT DES TRANSACTIONS

Article 13 : Règlement des soldes des systèmes monétiques

Les soldes de compensation des transactions des systèmes monétiques sont réglés dans les comptes de règlement ouverts en les livres de la Banque Centrale.

Article 14 : Règlement des soldes de compensation des transactions des institutions financières non bancaires

En vue du règlement de leurs soldes de compensation, les institutions financières non bancaires n'ayant pas de compte de règlement ouvert en les livres de la Banque Centrale concluent, à cette fin, des accords avec les banques commerciales qui en disposent.

Article 15 : Règlement des transactions WEB

Le règlement d'une transaction sur le Web doit être effectué sur le compte marchand sur une base J + 1 par l'acquéreur.

Article 16 : Traçabilité

L'opérateur enregistre les opérations à toutes les étapes de leur traitement, en particulier à l'entrée et à la sortie du système monétique. Le système monétique est doté d'une piste d'audit permettant de retracer toutes les actions qui y ont été réalisées.

L'opérateur est tenu de formaliser, enregistrer et surveiller les interventions manuelles dans le système monétique.

L'opérateur doit s'assurer que le système monétique enregistre immédiatement les erreurs dans le traitement des données et les perturbations affectant le système. Il met en place un cadre de gestion des incidents régulièrement mise à jour.

Article 17 : Plan de continuité

L'opérateur met en place un plan de continuité d'activités conforme à la norme ISO/IEC/22301.

Le plan de continuité d'activités prévoit au minimum le recours à un site de secours, des procédures ainsi que des ressources humaines et techniques pour garantir la continuité des opérations.

L'opérateur met en place un comité de crise pour gérer les incidents graves et assurer l'information des participants et des autres parties intéressées.

CHAPITRE II : CYBERSECURITE

Article 18 : Norme de sécurité minimale de l'environnement monétique de l'opérateur et du participant.

Tout opérateur et participant d'un système monétique doit certifier son environnement à la norme PCI-DSS et ISO/IEC/27001. Toute application qui traite les données du porteur devra être certifiée PA-DSS avant sa mise en service.

Article 19 : Accès et/ou maintien frauduleux

L'opérateur s'assure que le système monétique qu'il opère dispose des procédures et dispositifs visant à le protéger contre tout accès et/ou maintien frauduleux par des tiers non autorisées.

Article 20 : Atteinte à l'intégrité du système

L'opérateur prend toutes les dispositions nécessaires pour prévenir et contenir les attaques informatiques visant à entraver ou fausser le fonctionnement du système monétique dont il assure la gestion.

Article 21 : Atteinte à l'intégrité des données

L'opérateur prend toutes les dispositions requises pour protéger le système monétique contre l'introduction, la modification, et la suppression des données par des personnes non autorisées.

Article 22 : Centre de contrôle des opérations

L'opérateur se dote d'un centre de contrôle des opérations assurant en permanence 24h/24 et 7j/7 le contrôle des activités des utilisateurs et des accepteurs des cartes afin de permettre une réaction efficace contre la fraude ou tout autre risque inhérent aux opérations monétiques.

Article 23 : Centre opérationnel de sécurité

L'opérateur se dote d'un centre opérationnel de sécurité permettant de visualiser l'état du trafic, les incidents et les tentatives d'attaques sur le système monétique.

L'opérateur peut externaliser son centre opérationnel de sécurité. Dans ce cas, il demeure responsable de la réalisation, par son sous-traitant, des diligences visées à l'alinéa précédent.

Les cas de fraude avérée ou présumée, les attaques informatiques ainsi que les mesures prises par l'opérateur pour leur gestion sont portés à la connaissance de la Banque Centrale dans les 48 heures suivant leur constatation.

CHAPITRE III : TARIFICATION

Article 24 : Tarification

Les opérateurs communiquent à la Banque Centrale, durant la première semaine de chaque semestre et à l'occasion de toute modification, les conditions tarifaires appliquées pour les opérations monétiques.

Article 25 : Frais de contrôle

La Banque Centrale peut percevoir des frais de contrôle dans le cadre de la surveillance des systèmes monétiques et des services connexes, conformément aux Tarifs et conditions des opérations de la Banque Centrale.
Les opérateurs des systèmes de paiement ayant qualité de banque sont exemptés du paiement des frais de contrôle pour la surveillance des systèmes monétiques.

S'agissant des Opérateurs des Banques qui ne sont rien d'autres que les Banques commerciales, pour éviter le double changement, la Banque Centrale du Congo opère un seul prélèvement des frais couvrant la surveillance des Systèmes et instruments de paiement ainsi que la Supervision des Intermédiaires Financiers.

CHAPITRE IV : OBLIGATIONS D'INFORMATION

Article 26 : Reporting et communication

Les opérateurs transmettent mensuellement à la Banque Centrale les informations ci-après:

- les statistiques des transactions traitées dans le système en volume et en valeur ;
- l'état de la compensation et des règlements ;
- l'état des rejets techniques et financiers ;
- les données relatives à la fraude ;
- les informations sur les changements techniques éventuels ;
- toute autre information que la Banque Centrale estime nécessaire.

Les prestataires des services connexes et les émetteurs sont tenus à la même obligation sauf en ce qui concerne l'état de la compensation et des règlements.

Les opérateurs, les prestataires des services connexes et les émetteurs déclarent immédiatement à la Banque Centrale les incidents survenus dans un délai de deux jours et lui transmettent dans les cinq jours à dater de la déclaration un rapport détaillé sur lesdits incidents comprenant notamment la nature, la durée, l'origine et l'impact des incidents ainsi que les mesures adoptées pour leur prise en charge.

Article 27 :Confidentialité des données

Les opérateurs, les prestataires des services connexes et les émetteurs ne divulguent aucune information confidentielle dont ils ont connaissance.
Toutefois, cette divulgation est permise dans les cas ci-après :

- le consentement du participant, du client et de la personne concernée ;
- les réquisitions de la Banque Centrale, de l'administration fiscale ou des autorités judiciaires.

TITRE IV : NORMES APPLICABLES AUX GAB, DAB, TPE, SERVICES WEB ET A LA C ARTE DE PAIEMENT

CHAPITRE I[er] : NORMES SUR LES GAB ET DAB

Article 28 : Exigences minimales pour les GAB et DAB

Les GAB et DAB opérationnels en République Démocratique du Congo doivent remplir les conditions ci-après :

- les GAB et DAB doivent se conformer aux normes PCI DSS et EMV ;
- les GAB et DAB doivent être en mesure de distribuer dans n'importe quelle dénomination des billets ayant cours légal en République Démocratique du Congo ;
- les GAB et DAB sont dotés d'une piste d'audit et des capacités de journalisation complète des opérations monétiques ;
- les GAB et DAB doivent afficher clairement le logo des réseaux d'acceptation dont ils font partie.

Article 29 : Déploiement des GAB et DAB

Les aspects de déploiement et de sécurité suivants sont à respecter :

a) les GAB et DAB doivent être équipés de caméras qui enregistrent les personnes qui les utilisent ainsi que toutes les activités qui s'y déroulent. Ces enregistrements sont conservés pendant une période de six mois;
b) les caméras de surveillance ne doivent pas permettre la visualisation et l'enregistrement de la saisie des PIN;
c) les caméras de surveillance sont fixées solidement à une hauteur qui ne soit pas facile d'accès pour éviter toute manipulation, dommage ou compromission ;
d) les réseaux utilisés pour la transmission des transactions effectuées au moyen des GAB et DAB doivent permettre de préserver la confidentialité, la disponibilité et l'intégrité des données. Des mesures de précaution doivent être prises pour éviter toute intrusion frauduleuse au réseau du GAB et DAB ;
e) les participants doivent mettre en place des mesures garantissant la sécurité physique des utilisateurs des GAB et DAB ;
f) les GAB et DAB doivent être installés dans des endroits garantissant la sécurité des utilisateurs ;
g) les GAB et DAB doivent être solidement fixés de sorte à empêcher leur extraction frauduleuse ;

h) les GAB et DAB doivent être suffisamment et constamment éclairés pour assurer une bonne visibilité ;
i) les informations affichées sur les GAB et DAB doivent être suffisamment lisibles et intelligibles. Les GAB et DAB doivent permettre au moins l'affichage des informations en langue française ;
j) les GAB et DAB doivent être placés à l'abri des intempéries ;
k) les circuits d'alimentation électrique des GAB et DAB doivent être isolés et protégés pour éviter les chocs électriques ou l'électrocution ;
l) les GAB et DAB doivent être dotés d'une alimentation électrique de secours de manière à ce qu'ils ne cessent pas de fonctionner en cours d'une transaction.

Article 30 Opérations des GAB et DAB

Les transactions effectuées au moyen des GAB et DAB sont réalisées conformément aux règles suivantes :

a) les SLA spécifient que la durée de maintenance préventive des GAB et DAB ne dépasse pas 24 heures
b) en cas de panne des GAB et DAB, les participants sont tenus de remonter l'information à l'opérateur endéans 48 heures suivant le constat de la panne ;
c) les contacts du service d'assistance du participant sont affichés sur les GAB et DAB. La Banque garantit que son service d'assistance est fonctionnel 24 heures/24 et 7 jours/7 ;
d) tous les frais perçus pour les transactions effectuées au moyen des GAB et DAB doivent être divulgués aux clients avant leur réalisation. Les GAB et DAB doivent permettre au client de recevoir, à sa demande, un reçu de la transaction effectuée, indiquant au minimum le montant, les frais, la date et l'heure de la transaction. Le reçu de la transaction doit être lisible et intelligible ;
e) en l'absence du reçu de la transaction, les GAB et DAB doivent permettre au client de choisir de poursuivre ou non la transaction ;
f) les modules de distribution, de dépôt et de recyclage des GAB et DAB doivent être en bon état de fonctionnement ;
g) le module de distribution doit présenter les billets au client pendant 20 secondes au maximum, avant de les rétracter. Dans ce dernier cas, le montant rétracté est porté au crédit du compte du client ;
h) un mécanisme de monitoring en ligne approprié est mis en place pour suivre le bon fonctionnement des GAB et DAB ;

i) un mécanisme de monitoring en ligne est mis en place pour suivre le niveau de trésorerie des cassettes des GAB et DAB. Une alerte de seuil minimum des espèces est déclenchée afin d'assurer le réapprovisionnement des coffres forts des GAB et DAB et garantir, à tout moment, une disponibilité constante des espèces ;
j) les GAB et DAB sont approvisionnés avec des billets propres et ayant cours légal ;
k) des participants peuvent se convenir des modalités d'approvisionnement et de maintenance de leurs GAB et DAB ;
l) les acquéreurs et émetteurs sont astreints à l'obligation de vigilance dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme. Les transactions suspectes doivent être rapportées à la Cellule Nationale de Renseignements Financiers et à la Banque Centrale ;
m) tout participant est tenu de disposer d'un registre reprenant tous ses GAB et DAB et renseignant notamment leur emplacement, leur identification et leur numéro de série ;
n) les GAB et DAB ne doivent pas afficher le PIN et le numéro de la carte de paiement pour réduire les risques de fraude ;
o) des précautions doivent être prises pour minimiser le risque d'oubli de la carte de paiement dans les GAB et DAB, à travers un message sonore alertant le client de retirer sa carte ;
p) la carte de paiement doit être éjectée du GAB ou DAB avant la sortie des billets de banque, pour réduire le risque de son oubli.

Article 31 : Maintenance des GAB et DAB

Un avis au public est affiché pendant la période d'interruption du service des GAB et DAB en raison d'une maintenance planifiée.

Les participants réalisent la maintenance de leurs GAB et DAB conformément aux indications du fournisseur.

Article 32 : Inspections des GAB et DAB

Les participants réalisent des inspections de leurs GAB et DAB au moins une fois par trimestre. Ces inspections sont consignées dans un registre pouvant être consulté par la Banque Centrale.

Le registre ou journal de maintenance des GAB et DAB est conservé correctement dans des conditions garantissant son intégrité.

CHAPITRE II : NORMES SUR LES SERVICES D'ACCEPTATION SUR TPE

Article 33 : Types de TPE

Les équipements ci-après sont considérés comme des terminaux de paiement électronique :

a) les terminaux de paiement par carte de paiement ;
b) le téléphone et les TPE mobiles ;
c) les distributeurs automatiques de carburant ;
d) les distributeurs automatiques de jeton ;
e) les terminaux de paiement biométrique ;
f) les terminaux de paiement sans contact.

Article 34 : Connectivité

Les options de connectivité TPE incluent, sans s'y limiter :

a) Ethernet / RS 232 ;
b) GPRS ou plus ;
c) Bluetooth ou wifi ;
d) Communication en champ proche (Near-Field Communication ou NFC).

Article 35 : Parties prenantes des services d'acceptation

Les parties prenantes des services d'acceptation des cartes de paiement ou tout autre procédé de transfert électronique de fonds sur TPE sont :

a) les acquéreurs ;
b) les émetteurs ;
c) les accepteurs ;
d) les porteurs ;
e) Le système de paiement ou Switch monétique.

Article 36 : Standards applicables

Les TPE, applications et systèmes de traitement des transactions monétiques doivent répondre aux standards suivants :

a) EMV ;
b) PCI-DSS ;
c) PCI P2PE ;
d) PCI-PED ;
e) Triple-DES/RSA.

La conformité aux standards évoqués à l'alinéa 1er est attestée par des certificats à jour délivrés par les organismes qui les ont édictés.

Article 37 : Rôles et responsabilités des acquéreurs

L'acquéreur conclut avec l'accepteur un contrat devant énoncer clairement les termes et conditions d'utilisation du TPE, les droits des parties et leurs responsabilités, notamment en matière de maintenance des TPE.

En outre, les acquéreurs :

a) s'assurent que les TPE achetés et déployés auprès des accepteurs acceptent toutes les cartes de paiement du réseau d'acceptation ;
b) assurent la formation des accepteurs et mettent en place des processus ainsi que des dispositifs permettant de vérifier l'identité du porteur et de détecter toute utilisation suspecte, frauduleuse ou non autorisée des instruments de paiement électronique ;
c) sont tenus de prendre des mesures pour empêcher l'utilisation de leurs réseaux à des fins de fraude, de blanchiment des capitaux et du financement du terrorisme ainsi que d'autres délits financiers ;
d) fournissent aux accepteurs des lignes directrices sur les procédures de paiement pour les transactions de grande valeur.

CHAPITRE III : SERVICE D'ACCEPTATION WEB

Article 38 : Normes minimales

L'acquéreur doit utiliser les services d'un système de paiement qui respecte les normes minimales suivantes :

- PCI DSS;
- 3-D sécure.

Article 39 : Parties prenantes

Les intervenants du service d'acceptation Web sont notamment :

- l'acquéreur ;
- l'émetteur ;
- l'accepteur ;
- le gestionnaire de la plateforme de e-commerce ;
- le porteur ;
- le système de paiement ou le switch monétique.

Article 40 : Responsabilités de l'acquéreur

L'acquéreur assume les responsabilités suivantes :

a) disposer d'une plateforme d'e-commerce ou recourir au service d'un prestataire tiers, gestionnaire d'une plateforme d'e-commerce en répondant des prestations de ce dernier ;
b) intégrer le site web de l'accepteur dans la plateforme d'e-commerce ;
c) catégoriser l'accepteur et définir les limites des transactions ;
d) s'assurer que l'accepteur effectue régulièrement une analyse des menaces sur son site web et fournit des mises à jour sur les menaces émergentes ;
e) s'assurer que les données confidentielles du client ne sont pas stockées sur le site web de l'accepteur ;
f) signer un accord avec l'accepteur afin de recevoir les paiements effectués sur son site web ;
g) respecter son obligation de vigilance dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme. Les transactions suspectes doivent être rapportées à la Cellule Nationale de Renseignements Financiers et à la Banque Centrale ;
h) interrompre ses prestations notamment en cas d'opérations suspectes ou de fraude ;
i) mettre en place les procédures de règlement applicables en situation ordinaire et de crise ;
j) mettre en place les procédures de gestion des risques.

Article 41 : Responsabilités de l'accepteur

L'accepteur assume les responsabilités suivantes:

a) afficher clairement les termes et les conditions de vente ou livraison des biens ainsi que les prestations de service sur son site web ;
b) coopérer avec l'acquéreur dans la mise en œuvre des mesures de sécurité du site web ;
c) fournir au client des instructions sur le processus de paiement et de tous les frais applicables ;
d) analyser les menaces émergentes et prendre des précautions pour éviter leur survenance.

Article 42 : Responsabilités de l'émetteur

L'émetteur assume les responsabilités suivantes:

a) émettre des cartes de paiement, physique ou virtuelle ;
b) émettre la monnaie électronique ;
c) ouvrir et autoriser l'approvisionnement des comptes courant ou virtuels ;
d) autoriser la transaction du porteur ;
e) prendre des mesures de sécurité nécessaires contre notamment toute fraude ou toute opération irrégulière ;
f) fournir des moyens par lesquels un porteur peut l'informer d'une perte, d'un vol ou d'une utilisation frauduleuse d'une carte de paiement ;
g) conserver les documents sur une période minimale de cinq ans ;
h) définir des limites globales de transaction par canal et par jour ;
i) gérer les procédures de chargebacks des porteurs.

Article 43 : Responsabilités du gestionnaire de la plateforme de e-commerce

Le gestionnaire de la plateforme de e-commerce assume les responsabilités suivantes :

a) traiter la transaction de paiement en ligne ;
b) agir en tant que facilitateur pour le compte de l'accepteur afin de permettre la transaction ;
c) être responsable de la sécurité des données de paiement qui sont sous sa gestion ;
d) faire l'objet d'audit de sécurité.

CHAPITRE IV : NORMES APPLICABLES A LA CARTE DE PAIEMENT

Article 44 : Modèle de la carte de paiement

Toute carte de paiement, physique ou virtuelle, émise en République Démocratique du Congo doit être conforme :

- aux standards EMV ;
- à la norme ISO/CEI 7816 pour la carte de paiement avec contact ;
- à la norme ISO/CEI 14443 pour la carte de paiement sans contact.

Article 45 : Dimensions de la carte

Toute carte de paiement émise en République Démocratique du Congo doit se conformer aux métriques reprises à l'annexe de la présente instruction.

TITRE V : SANCTIONS

Article 46 : Mesures disciplinaires

Lorsque les opérateurs, les participants, les émetteurs et les acquéreurs contreviennent aux dispositions de la présente Instruction, la Banque Centrale, sans préjudice des dispositions légales, peut prendre les mesures suivantes:

- le rappel à l'ordre ;
- le blâme ;
- la suspension ;
- le retrait d'autorisation ou d'agrément;
- les amendes administratives définies dans les Tarifs et conditions des opérations de la Banque Centrale.

TITRE VI : DISPOSITIONS TRANSITOIRES ET FINALES

Article 47 : Dispositions transitoires

Les opérateurs des systèmes monétiques et les prestataires des services connexes disposent d'une période de 6 mois pour se conformer aux dispositions de la présente instruction. A cet effet, ils sont tenus de transmettre trimestriellement à la Banque Centrale/Direction des Systèmes de Paiement, un rapport détaillé sur l'état de mise en œuvre des exigences de la présente instruction.

Article 48 : Entrée en vigueur

La présente Instruction entre en vigueur à la date de sa signature.

Fait à Kinshasa, le 09 MARS 2020

Déogratias MUTOMBO MWANA NYEMBO
Gouverneur

ANNEXE SUR LA DIMENSION DE LA CARTE DE PAIEMENT