

19 DEC 2006

**Instruction N° 05/2006 portant mise en application des règles de certification bancaire prévue par l'ordonnance 2006-031 relative aux instruments de paiements et aux opérations du commerce électroniques.**

**Le Gouverneur de la Banque Centrale de Mauritanie ;**

- Vu la loi n° 73.118 du 30 mai 1973 portant création de la BCM et fixant ses statuts modifiés par la loi n° 74.118 du 8 juin 1974 et la loi n° 75.332 du 26 décembre 1975 ;
- Vu la loi n° 95.011 du 17 Juillet 1995, abrogeant et remplaçant l'ordonnance n°91.042 du 30 décembre 1991, portant réglementation bancaire ;
- Vu l'Ordonnance n° 031.2006 du 23 Août 2006 relative aux instruments et opérations du commerce électroniques ;
- Vu la loi 2004-042 du 26 juillet 2004 fixant le régime applicable aux relations financières avec l'étranger et à leur enregistrement statistique ;
- Vu le décret n°110-2006 du 13 Septembre 2006 portant nomination du Gouverneur de la Banque Centrale de Mauritanie.

**DECIDE :**

**CHAPITRE 1 : DISPOSITIONS GENERALES**

**Article 1 : Définitions :**

Les termes employés dans la présente instruction s'entendent comme suit :

**CCB :** Comité de Certification Bancaire placé sous la tutelle de la Banque Centrale et chargé de la certification des signatures électroniques des émetteurs ;

**Clé :** Une suite de symboles permettant les opérations de chiffrement et de déchiffrement.

**Certificat électronique :** un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;

**Signature électronique :** La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

**Emetteur de signature électronique :** banque ou institution financière autorisée par la loi à produire des instruments de paiements. Il désigne également tout groupement de ces personnes morales autorisé par la Banque Centrale. Il s'agit également de toute personne qui met en oeuvre un dispositif de création de signature électronique ;

**Données de création de signature électronique :** les éléments propres au signataire, tels que des clés cryptographiques publiques, utilisés pour créer la signature électronique ;

**Dispositif de création de signature électronique :** un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;

**Données de vérification de signature électronique :** les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;

**Dispositif de vérification de signature électronique :** un matériel ou logiciel destiné à mettre en application les données de vérification de signature électronique ;



### **Article 2 : Objet**

L'objet de la présente instruction est de régir les règles d'application relatives à la certification bancaire pour l'émission des cartes.

La sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée en matière de transactions bancaires et financières peut être certifiée dans les conditions prévues par la présente Instruction.

### **Article 3 : Cryptographie**

Dans le respect des régimes des moyens et prestations de cryptographie, des matériels et logiciels, offrant un service de confidentialité mis en oeuvre par un algorithme à clé de longueur supérieure ou égale à 1024 bits, peuvent être utilisés pour les besoins de la sécurité des transactions bancaires et financières.

## **CHAPITRE 2 : DU COMITE DE CERTIFICATION BANCAIRE**

### **Article 4 : Création et organisation**

Il est créé au sein de la Banque Centrale, un Comité de Certification Bancaire dénommée (CCB). Le CCB est rattaché au cabinet du Gouverneur de la Banque Centrale.

Les missions du CCB se limitent aux domaines bancaire et financier. A cet effet, Il est chargé de :

1. L'émission, la délivrance et la conservation des certificats électroniques ;
2. Le contrôle du respect par le fournisseur de services de signature électronique des dispositions en vigueur ;
3. La fixation des caractéristiques du dispositif de création et de vérification de la signature ;
4. La participation aux activités de recherche, de formation et d'étude afférentes aux échanges électroniques ;
5. Et d'une manière générale, toute autre activité en rapport avec son domaine d'intervention.

Une note de service fixera l'organisation de ce Comité de certification bancaire ainsi que les personnes qui seront affectées au sein de ce Comité.

## **CHAPITRE 3 : REGLES RELATIVES A LA CERTIFICATION**

### **Article 5 : Condition de certification**

Toute personne morale désireuse d'obtenir un certificat pour l'émission de transactions électroniques doit satisfaire les conditions suivantes :

- être i) une banque agréée conformément aux dispositions légales ii) ou une institution autorisée à proposer des services financiers ;
- et avoir fait l'objet d'un audit de sécurité des locaux et des équipements informatiques et techniques destinés à ces activités.

Cet audit de sécurité est fait par la Banque Centrale ou un tiers qu'elle a délégué. A défaut de notification d'opposition dans les trente jours qui suivent la fin de cet audit, la personne morale est automatiquement autorisée à émettre des signatures électroniques dans le domaine bancaire et financier.



**Article 6 : Recours aux tiers**

Pour appuyer le Comité de certification bancaire, la Banque Centrale peut recourir aux prestations de ses services ou à celles des tiers nationaux ou étrangers en vue de l'évaluation, de la certification et de la qualification des fournisseurs de services liés à la signature électronique opérant dans le domaine bancaire et financier.

**Article 7 : Publicité de la liste des organismes accrédités**

Le Comité de certification bancaire est tenu de mettre à la disposition du public la liste des organismes accrédités par la Banque Centrale. La publication de cette liste peut aussi être faite sur un site Internet. Cette liste est tenue à jour.

**Article 8 : Durée du certificat**

Le certificat est accordé pour une période de deux ans à compter de sa date de délivrance. Il peut être renouvelé.

**Article 9 : Autorisation pour tout changement**

L'émetteur doit avertir le CCB de tout projet de changement relatif aux informations sur la base desquelles le certificat a été délivré.

Le Comité de certification bancaire doit, dans un délai n'excédant pas quinze jours, notifier au titulaire sa réponse. En cas de changement sans accord, le CCB devra se prononcer sur la validité du certificat.

**Article 10 : Certification des données**

La certification est faite par le Comité de certification bancaire. Elle atteste que l'exemplaire du produit ou du système soumis à vérification répond aux caractéristiques de sécurité spécifiées. Elle atteste également que la vérification a été conduite conformément aux règles et procédures en vigueur.

**Article 11 : Reconnaissance de certificats étrangers**

Les certificats délivrés par un réseau international auquel les émetteurs ou leur groupement sont affiliés ont la même valeur juridique que ceux délivrés par le CCB.

**CHAPITRE 4 : DES PROCEDURES DE CERTIFICATION****Article 12 : Objet**

Le présent chapitre décrit les différents échanges entre le CCB et les émetteurs en vue de la certification liée à la signature électronique.

**Article 13 : Préparations des données du CCB**

Préalablement à toute demande de certification, le CCB génère une bi-clé RSA (une clé publique et une clé privée). La clé publique auto signée par le Comité de certification bancaire, est envoyée à l'émetteur.

**Article 14 : Transmission des clés**

L'envoi de la clé publique du CCB est réalisé sous la forme de deux fichiers distincts :

- ⇒ **SID.Vnk** (nom du fichier par défaut): Informations concernant la clé du Comité de Certification bancaire transmises à l'émetteur. Il contient la clé publique concaténée avec un certificat signé par la clé privée du CCB.



⇒ **SID.Hnk** (nom du fichier par défaut): il contient l'empreinte du certificat de la clé publique du Comité de Certification Bancaire.

La transmission des fichiers s'effectue toujours par des canaux distincts.

#### **Article 15: Contenu des clés du CCB**

Le fichier de la clé publique contient obligatoirement la concaténation du bloc de données (attributs de la clé publique du CCB, certificat auto signé de la clé du CCB), la référence et le chiffrement.

#### **Article 16: Préparations des données émetteurs**

Pour cette phase, l'émetteur génère, lui aussi, une bi-clé RSA (une clé publique et une clé privée). La clé publique et la demande de certificat émetteur sont envoyées au CCB.

#### **Article 17: Demande de certificat émetteur**

Le formulaire de la demande de certificat émetteur est, au préalable, envoyé au CCB sans « tracking number » qui est attribué par le CCB. Dans un second temps, l'envoi des fichiers se fait avec le « tracking number » rappelé dans le nom du fichier.

La demande de l'émetteur est accompagnée d'un formulaire contenant les informations suivantes (formulaire joint en annexe) :

- SID (Service Identifier) ;
- Bank Identification Number (BIN) ;
- Date d'expiration du certificat ;
- Tracking number (à remplir par le CCB) ;
- Longueur du modulo de la clé émetteur (en octets, exprimé en décimal) ;
- Exposant public de la clé émetteur.

#### **Article 18: Mode d'envoi de la demande**

L'envoi de la demande de certificat au CCB qui se fait sous deux canaux différents, est réalisé sous la forme de deux fichiers distincts :

- **SID.Ink** (nom du fichier par défaut): Informations concernant la clé de l'émetteur transmises au Comité de Certification Bancaire. Il contient la clé publique et ses attributs concaténé avec un certificat signé par la clé privée de l'émetteur.
- **SID.Hnk** (nom du fichier par défaut): il contient l'empreinte du certificat de la clé publique de l'émetteur.

#### **Article 19: Contenu des clés émetteur**

Le fichier de la clé publique émetteur contient obligatoirement la concaténation du bloc de données (attributs de la clé publique émetteur, certificat auto-signé de la clé de l'émetteur), la référence et le chiffrement.

#### **Article 20: Signature et envoi de la clé**

Le CCB signe la clé publique de l'émetteur avec sa clé privée et génère un certificat de clé publique de l'émetteur. Ce certificat est retourné à l'émetteur ou à une tierce personne dûment autorisée.

Le certificat délivré par le CCB peut être transmis par mail dans la mesure où son intégrité et son origine sont garanties par la signature de la Banque Centrale.



**Article 21: Contenu du certificat émetteur délivré par le CCB**

Le fichier du certificat de la clé publique émetteur contient obligatoirement la concaténation du bloc de données (attributs de la clé publique de l'émetteur, clé publique signée par le CCB, signature du message de réponse du CCB), la référence et le chiffrement.

**Article 22 : Validation du certificat par l'émetteur**

L'émetteur vérifie la validité de son certificat reçu en utilisant la clé publique du Comité de certification bancaire. Si le certificat est correct, l'émetteur peut l'inclure dans les données de personnalisation de ses cartes à puce.

**Article 23 : Contenu du certificat électronique**

Les données techniques relatives au certificat électronique comprennent notamment :

- l'identité du titulaire du certificat
- l'identité de la personne qui l'a émis et sa signature électronique,
- les éléments de vérification de la signature du titulaire du certificat,
- la durée de validité du certificat,
- les domaines d'utilisation du certificat

**Article 24 : Confidentialité des informations**

Le CCB ainsi que les personnes qui concourent à la réalisation de sa mission, doivent garder secrètes les informations confiées à eux dans le cadre de l'exercice de leurs activités à l'exception de celles dont la publication ou la communication ont été autorisées par écrit sous support papier ou par voie électronique par le titulaire du certificat électronique ou dans les cas prévus par la législation en vigueur.

En cas de demande de certification, le CCB collecte les informations nécessaires directement auprès de la personne concernée ou, moyennant son accord écrit ou électronique, auprès des tiers.

Dans le cadre de sa mission de certification, il est interdit au CCB de :

- collecter les informations non nécessaires à la certification de la signature électronique ;
- utiliser, en dehors du cadre de ses activités, les données ou informations qu'il a collectées pour la certification de la signature électronique sans avoir obtenu l'accord écrit ou électronique de la personne concernée.

**Article 25 : Obligation d'information**

Le CCB doit tenir un registre électronique des certificats délivrés accessible en permanence pour consultation électronique des informations qui y sont enregistrées. Le registre des certificats, régulièrement mis à jour, doit être protégé contre toute modification non autorisée.

**Article 26 : Obligations de garantie**

Le CCB garantit :

- l'exactitude des informations contenues dans le certificat électronique à la date de sa délivrance ;
- le lien entre le titulaire du certificat électronique et le dispositif de vérification de signature qui lui est propre ;
- la détention par le titulaire du certificat électronique d'un dispositif de création de signature conforme aux dispositions en vigueur.



**Article 27 : Responsabilités du titulaire du certificat électronique**

Dès le moment de la préparation des données afférentes à la création du certificat, l'émetteur est responsable de :

1. la confidentialité des données afférentes à la création de certificat. En cas de doute quant au maintien de la confidentialité des données afférentes à la création du certificat ou de perte de conformité à la réalité des informations fournies au CCB, l'émetteur est tenu de faire annuler le certificat ;
2. l'utilisation de ces données ;
3. tout retard dans la fourniture de l'information à toute personne morale dont on peut raisonnablement penser qu'elle se fiera à cette certification et offrira des services utilisant cette certification ;
4. toute négligence dans la prise de dispositions raisonnables pour garantir l'exactitude et l'exhaustivité de toutes les déclarations faites par lui pour étayer sa demande de certification.

Le titulaire du certificat électronique engage sa responsabilité pour toute violation de la confidentialité et de l'intégrité de son dispositif de création de signature électronique.

Le titulaire du certificat électronique est tenu de notifier au CCB toute modification des informations fournies.

**Article 28 : Responsabilités de la Banque Centrale**

La responsabilité de la Banque centrale peut être engagée si sa faute ou sa négligence peut être prouvée par le titulaire du certificat ayant subi un préjudice.

En cas de retrait ou de suspension de l'agrément d'une institution financière membre du système de paiement interbancaire du GIMTEL, la BCM fournit immédiatement cette information à ce dernier en vue de la radiation du certificat de cette institution sur la liste du système de paiement.

**Article 29 : Fin du Certificat**

Lorsqu'un certificat électronique est arrivé à échéance ou a été annulé, le titulaire de celui-ci ne doit plus utiliser les données afférentes à ce certificat.

La suspension ou la révocation du certificat peut survenir en cas de réalisation de faits ou d'actes pouvant porter atteinte à la sécurité du système de paiement électronique notamment en cas d'erreur, de falsification, de violation du dispositif de création de signature, de fraude de certificat, de perte d'agrément ou de changement d'informations.

Le titulaire du certificat désirant suspendre ou révoquer celui-ci est tenu de faire une demande adressée auprès du CCB. Après réception et traitement confirmant l'identité du titulaire, le CCB procède à la suspension ou à la révocation du certificat sur son registre et communique immédiatement au GIMTEL ou à toute structure technique compétente l'information en vue de la radiation du certificat du système de paiement électronique.

**Article 30 : Accès information**

Le titulaire du certificat électronique peut, à tout moment, par demande signée par écrit ou par voie électronique obtenir une copie des informations le concernant.



## **CHAPITRE 5 : DU CONTROLE ET DES SANCTIONS**

### **Article 31 : Pouvoirs de contrôle et de sanction**

Le CCB détermine les règles relatives au contrôle des émetteurs certifiés.

Le Comité de certification bancaire peut exercer, d'office ou à l'occasion d'une réclamation mettant en cause l'activité d'un émetteur certifié, un contrôle sur place et / ou sur pièces.

En cas de manquement aux dispositions de la présente instruction et sans préjudice des sanctions légales, la Banque Centrale peut, en fonction de la gravité de l'acte, prendre les sanctions administratives suivantes :

- amende de 50.000 UM à 500.000 d'ouguiya ;
- Suspension provisoire de un à douze mois pour l'exercice de certaines activités ;
- Annulation du certificat ;
- En de récidive ou en fonction de la gravité de l'acte, engager la procédure de retrait des équipements utilisés.

### **Article 32 : Entrée en vigueur**

La présente instruction prend effet à compter de sa date de signature.

Nouakchott le

**OUSMANE KANE**





**ANNEXE : Formulaire de demande de certification**

<b>SID (Service Identifier)</b>	
<b>BIN</b>	
<b>Date d'expiration du certificat</b>	
<i>Tracking number (à remplir par le CCB)</i>	
<b>Longueur du modulo de la clé émetteur (en octets, exprimé en décimal)</b>	
<b>Exposant public de la clé émetteur</b>	



## Table des matières

CHAPITRE 1 : DISPOSITIONS GENERALES .....	1
ARTICLE 1 : DEFINITIONS : .....	1
ARTICLE 2 : OBJET .....	2
ARTICLE 3 : CRYPTOGRAPHIE .....	2
 CHAPITRE 2 : DU COMITE DE CERTIFICATION BANCAIRE.....	2
ARTICLE 4 : CREATION ET ORGANISATION .....	2
 CHAPITRE 3 : REGLES RELATIVES A LA CERTIFICATION.....	2
ARTICLE 5 : CONDITION DE CERTIFICATION .....	2
ARTICLE 6 : RECOURS AUX TIERS .....	3
ARTICLE 7 : PUBLICITE DE LA LISTE DES ORGANISMES ACCREDITES .....	3
ARTICLE 8 : DUREE DU CERTIFICAT .....	3
ARTICLE 9 : AUTORISATION POUR TOUT CHANGEMENT .....	3
ARTICLE 10 : CERTIFICATION DES DONNEES .....	3
ARTICLE 11: RECONNAISSANCE DE CERTIFICATS ETRANGERS .....	3
 CHAPITRE 4 : DES PROCEDURES DE CERTIFICATION .....	3
ARTICLE 12 : OBJET .....	3
ARTICLE 13 : PREPARATIONS DES DONNEES DU CCB .....	3
ARTICLE 14 : TRANSMISSION DES CLES .....	3
ARTICLE 15: CONTENU DES CLES DU CCB.....	4
ARTICLE 16: PREPARATIONS DES DONNEES EMETTEURS .....	4
ARTICLE 17: DEMANDE DE CERTIFICAT EMETTEUR .....	4
ARTICLE 18: MODE D'ENVOI DE LA DEMANDE .....	4
ARTICLE 19: CONTENU DES CLES EMETTEUR .....	4
ARTICLE 20: SIGNATURE ET ENVOI DE LA CLE .....	4
ARTICLE 21: CONTENU DU CERTIFICAT EMETTEUR DELIVRE PAR LE CCB .....	5
ARTICLE 22 : VALIDATION DU CERTIFICAT PAR L'EMETTEUR .....	5
ARTICLE 23 : CONTENU DU CERTIFICAT ELECTRONIQUE .....	5
ARTICLE 24 : CONFIDENTIALITE DES INFORMATIONS.....	5
ARTICLE 25 : OBLIGATION D'INFORMATION .....	5
ARTICLE 26 : OBLIGATIONS DE GARANTIE .....	5
ARTICLE 27 : RESPONSABILITES DU TITULAIRE DU CERTIFICAT ELECTRONIQUE .....	6
ARTICLE 28 : RESPONSABILITES DE LA BANQUE CENTRALE.....	6
ARTICLE 29 : FIN DU CERTIFICAT .....	6
ARTICLE 30 : ACCES INFORMATION .....	6
 CHAPITRE 5 : DU CONTROLE ET DES SANCTIONS.....	7
ARTICLE 31 : POUVOIRS DE CONTROLE ET DE SANCTION .....	7
ARTICLE 32 : ENTREE EN VIGUEUR .....	7
 ANNEXE : Formulaire de demande de certification .....	8