REPUBLIQUE DU CAMEROUN

PAIX – TRAVAIL – PATRIE

**ARRETE N° 00000014 /MINPOSTEL DU 27 JUIN 2012**
**fixant les critères de qualification des certificats et les caractéristiques techniques du dispositif de création des signatures électroniques.-**

**LE MINISTRE DES POSTES ET TELECOMMUNICATIONS,**

Vu la Constitution ;

Vu la loi n° 98/013 du 14 juillet 1998 relative à la concurrence ;

Vu la loi n° 2001/010 du 23 juillet 2001 instituant le service minimum dans le secteur des télécommunications ;

Vu la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun ;

Vu la loi n° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun ;

Vu la loi n° 2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun ;

Vu la loi-cadre n°2011/012 du 6 mai 2011 portant protection des consommateurs au Cameroun ;

Vu le décret n°2005/124 du 15 avril 2005 portant organisation du Ministère des Postes et Télécommunications ;

Vu le décret n°2011/408 du 09 décembre 2011 portant organisation du Gouvernement;

Vu le décret n°2011/410 du 09 décembre 2011 portant formation du Gouvernement ;

Vu le décret 2012/180 du 10 avril 2012 portant organisation et fonctionnement de l'Agence Nationale des Technologies de l'Information et de la Communication ;

Vu le décret n°2012/1318/PM du 22 mai 2012 fixant les conditions et les modalités d'octroi de l'autorisation d'exercice de l'activité de certification électronique,

| SERVICES DU PREMIER MINISTRE VISA | |
|---|---|
| 008291 | 14 JUIN 2012 |
| PRIME MINISTER'S OFFICE | |

**ARRETE :**

**CHAPITRE I**
**DISPOSITIONS GENERALES**

**ARTICLE 1er**.- (1) Le présent arrêté fixe les critères de qualification des certificats et les caractéristiques techniques du dispositif de création des signatures électroniques.

(2) Il est pris en application des dispositions des articles 18, 20 alinéa 2 et 21 de la loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun.

**ARTICLE 2.-** Les certificats électroniques sont émis notamment pour la réalisation des opérations suivantes :

- l'identification de son titulaire ;
- l'attestation de la réalisation d'une transaction, ainsi que la fixation de sa date et de son horaire ;
- la réalisation des transactions électroniques.

**ARTICLE 3.-** Pour l'application du présent arrêté, les définitions ci-après sont admises :

1. **Algorithme** : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;

2. **Clé privée** : clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique), qui appartient à une entité et qui doit être secrète ;

3. **Clé publique** : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;

4. **Confidentialité** : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

5. **Dispositif de création de signature électronique** : ensemble d'équipements et/ou logiciels privés de cryptage, homologués par une autorité de certification accréditée, configurés pour la création d'une signature électronique ;

6. **Fiabilité** : aptitude d'un système d'information ou d'un réseau de communications électroniques à fonctionner sans incident pendant un temps suffisamment long.

## CHAPITRE II
## DES CRITERES DE QUALIFICATION DES CERTIFICATS ELECTRONIQUES

**ARTICLE 4.-** (1) Le certificat électronique est délivré par une autorité de certification électronique agréée.

SERVICES DU PREMIER MINISTRE
VISA
008291 / 14 JUIN 2012
PRIME MINISTER'S OFFICE

**ARTICLE 5**.- L'autorité de certification électronique est tenue d'émettre les certificats électroniques conformément aux normes prescrites par l'Agence Nationale des Technologies de l'Information et de la Communication, ci-après désignée « l'Agence ».

**ARTICLE 6**.- (1) Le certificat électronique contient les informations obligatoires suivantes :

- le niveau du certificat ;
- le code unique identifiant le certificat ;
- l'identité et l'adresse de l'autorité émettrice du certificat ;
- l'identifiant unique de l'autorité de certification ;
- l'identité de la personne physique ou la raison sociale de la personne morale titulaire du certificat ;
- le nom du domaine et l'identité du gestionnaire des serveurs, et le nom du domaine et l'identité du gestionnaire des réseaux ;
- la date du commencement et de péremption du certificat en jour, heure, minute, seconde et dixième selon l'horaire de Greenwich (GMT) ;
- l'identifiant unique du titulaire du certificat ;
- le dispositif de vérification de la signature du titulaire du certificat et les algorithmes y rattachés ;
- la signature électronique de l'autorité de certification et les algorithmes y rattachés ;



(2) Sans préjudice des dispositions de l'alinéa 1 ci-dessus, le certificat électronique peut également contenir les informations optionnelles prévues par les normes nationales et internationales en vigueur.

## CHAPITRE III

## DES CARACTERISTIQUES TECHNIQUES DU DISPOSITIF DE CREATION DES SIGNATURES ELECTRONIQUES

**ARTICLE 7**.- (1) Un dispositif sécurisé de création des signatures électroniques doit garantir par des moyens techniques et des procédures appropriées que les données de création de ladite signature sont :

- confidentielles et ne peuvent être établies plus d'une fois;
- protégées contre toute falsification et ne peuvent être trouvées par déduction;
- susceptibles d'être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

(2) Un dispositif sécurisé de création de signature électronique ne doit entraîner aucune altération du contenu de l'acte à signer, ni faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

**ARTICLE 8.**- Toute personne utilisant un dispositif de création de signature électronique doit :

- prendre les précautions minimales pour éviter l'utilisation illégale des éléments de cryptage ou des équipements personnels relatifs à sa signature ;
- informer l'autorité de certification de toute utilisation illégitime de sa signature ;
- veiller à la véracité de toutes les données qu'elle a déclarées à l'autorité de certification électronique et à toute personne à qui elle a demandé de se fier à sa signature.

ARTICLE 9.- (1) Toute personne désirant créer une signature électronique doit utiliser un dispositif comprenant :

- une paire de clés composée d'une clé privée utilisée pour la création de la signature et d'une clé publique utilisée pour la vérification de la signature ;

- un mot de passe ou tout autre procédé de sécurisation.

(2) La paire de clés visée à l'alinéa 1 ci-dessus est créée par un dispositif et des procédés fiables, en tenant compte du progrès technique dans le domaine, de l'unicité, de la longueur des clés créées et du niveau d'assurance de la confidentialité de la clé privée.

ARTICLE 10.- Le dispositif de création de paires de clés garantit notamment :

- la création des paires de clés sous une forme conforme aux normes en vigueur ;

- la conformité des paires de clés aux conditions des algorithmes de création et de vérification de la signature définie au cahier des charges des autorités de certification ;

- l'unicité des paires de clés.

ARTICLE11.- Les paires de clés sont uniques et personnelles. Elles ne sont ni cessibles, ni transférables à quelque titre que ce soit.

ARTICLE 12.- Le titulaire de la clé privée en garantit les conditions de sécurité et de protection.

ARTICLE 13.- (1) L'autorité de certification électronique contrôle l'accès au dispositif de création des clés.

(2) Elle identifie chaque utilisateur de ce dispositif et enregistre toutes les opérations réalisées par l'utilisation de ce dispositif dans un registre particulier.

SERVICES DU PREMIER MINISTRE
VISA
008291 / 14 JUIN 2012
PRIME MINISTER'S OFFICE

**ARTICLE 14**.- (1) Les paires de clés sont conservées obligatoirement auprès de l'autorité de certification électronique au moyen de tout procédé de sécurisation fiable.

(2) Elles sont divisées en plusieurs parties dont chacune est conservées auprès d'une entité différente des services de l'autorité de certification électronique.

**ARTICLE 15**.- (1) Le titulaire d'une clé et l'autorité de certification électronique utilisent un dispositif de signature qui permet de :

- conserver et d'utiliser la clé privée au moyen tout procédé de sécurisation fiable ;
- cacher la clé privée après chaque utilisation.

(2) En cas de perte de la clé privée, le titulaire en informe sans délai l'autorité de certification qui prend toutes les mesures appropriées.

**ARTICLE 16**.- (1) Les certificats utilisés par l'autorité de certification électronique sont classés, selon leurs fonctions, en trois catégories :

- les paires utilisées pour la création et la vérification de la signature électronique ;
- les paires utilisées pour la création et la vérification de la signature inscrite sur le certificat électronique et les registres y afférents ;
- les paires utilisées pour l'inscription de la date et de l'horaire.

(2) Les paires de clés visées à l'alinéa 1 ci-dessus ne peuvent être utilisées que pour les fonctions auxquelles elles sont dédiées.

## CHAPITRE IV
## DISPOSITION FINALE

**ARTICLE 17**.- Le présent arrêté sera enregistré, publié suivant la procédure d'urgence, puis inséré au Journal Officiel en français et en anglais./-

**Yaoundé le,** 27 JUIN 2012

**Le Ministre des Postes et Télécommunications,**

**Jean-Pierre BIYITI bi ESSAM**

SERVICES DU PREMIER MINISTRE
VISA
008291 / 14 JUIN 2012
PRIME MINISTER'S OFFICE

Pour le Ministre des Postes et Télécommunications
et Par Délégation
Le Secrétaire Général

Edouard Ebah Abada
ADMINISTRATEUR CIVIL
PRINCIPAL