PRESIDENCE DE LA REPUBLIQUE

SECRETARIAT GENERAL
DU GOUVERNEMENT

REPUBLIQUE DU CONGO
Unité*Travail*Progrès

Décret n° 2014 - 596 du 3 novembre 2014
portant réglementation de la signature électronique en matière d'échanges électroniques.

LE PRESIDENT DE LA REPUBLIQUE,

Vu la Constitution ;
Vu la loi n° 9-2009 du 25 novembre 2009 portant réglementation du secteur des communications électroniques ;
Vu la loi n° 16-2013 du 19 juillet 2013 portant création du guichet unique des opérations transfrontalières ;
Vu le décret n° 1035-2012 du 25 septembre 2012 portant nomination des membres du Gouvernement ;
Vu le décret n° 2014-77 du 6 mars 2014 portant approbation des statuts du guichet unique des opérations transfrontalières.

En Conseil des ministres,

DECRETE :

TITRE I : DISPOSITIONS GENERALES

Chapitre 1 : De l'objet

Article premier : Le présent décret a pour objet de faciliter l'utilisation des signatures électroniques, de contribuer à leur reconnaissance juridique et de fixer les conditions générales d'accréditation des prestataires de services, de certification des opérations ou des procédures, afin de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique en réseaux ouverts en matière d'économie numérique.

Chapitre 2 : Des définitions

Article 2 : Au sens du présent décret, on entend par :

- **signature électronique :** une donnée résultant de l'usage d'un procédé fiable d'identification qui garantit son lien avec l'acte auquel il s'attache. C'est un code

personnel comprenant des chiffres, des lettres ou des logos imprimés sur une carte à puce qu'il suffit d'insérer dans un lecteur connecté à un ordinateur pour opérer la signature ;

- **échanges électroniques** : les échanges qui s'effectuent en utilisant les documents électroniques ;
- **certificat électronique** : le document électronique sécurisé par la signature de la personne qui l'a émis et qui atteste après constat la véracité de son contenu ;
- **fournisseur de service de certification électronique** : toute personne physique ou morale qui émet, délivre, gère les certificats et fournit d'autres services associés à la signature électronique ;
- **dispositif de création de la signature électronique** : matériel et/ou logiciel destiné(s) à mettre en application les données de création de la signature électronique, comportant les éléments distincts caractérisant le signataire, tels que la clé cryptographique privée, utilisée par lui pour créer une signature électronique ;
- **cryptage** : l'utilisation des codes ou signaux non usuels permettant la conversion des informations à transmettre en des signaux incompréhensibles aux tiers ou l'utilisation de codes et de signaux indispensables à la lecture de l'information.

TITRE II : DU CARACTERE PROBANT ET DE LA VALIDITE DE LA SIGNATURE ELECTRONIQUE

Chapitre 1 : Du caractère probant de la signature électronique

Article 3 : Tout prestataire de services de certification a le droit d'utiliser les signatures électroniques créées dans les conditions de sécurité optimales telles que définies dans le présent décret.

Article 4 : La signature électronique a la même force probante que la signature manuscrite. Elle est opposable au juge, par défaut de preuve contraire.

En revanche, la valeur des autres signatures continuera à être appréciée par les juges.

Article 5 : La signature électronique réalisée sur la base d'un certificat qualifié de conformité et créée par un dispositif sécurisé de création, ne s'applique que si les certificats numériques ont été proposés par les autorités de certification accréditées par le guichet unique des opérations transfrontalières, en tant qu'autorité de certification racine de l'Etat congolais.

Chapitre 2 : De la validité de la signature électronique

Article 6 : Est nulle toute signature électronique élaborée dans des conditions autres que celles définies ci-après, relatives aux certificats, aux tiers de certifications et au processus de la signature électronique.

Article 7 : Sous peine de nullité, le certificat qualifié de conformité que doit fournir le prestataire de services de certification accrédité, doit contenir :

- une mention indiquant que le certificat est délivré à titre de certificat qualifié de conformité ;
- l'identification du prestataire de service de certification, ainsi que le pays dans lequel il est établi ;
- le nom du signataire ;
- les données afférentes à la vérification de signature qui correspondent aux données pour la création de la signature sous le contrôle du signataire ;
- l'indication du début et de la fin de la période de validité du certificat ;
- le code d'identité du certificat ;
- la signature avancée du prestataire de service de certification qui délivre le certificat.

Le titulaire du certificat peut être une personne physique ou morale.

Article 8 : Les tiers de certification ou les fournisseurs de services de certification (autorité secondaire) doivent obtenir l'agrément auprès du guichet unique des opérations transfrontalières et conserver l'accréditation par le guichet unique des opérations transfrontalières dans les cas suivants :

- faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification ;
- assurer le fonctionnement d'un service d'annuaire rapide et sûr ainsi que d'un service de révocation sûr et immédiat ;
- veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;
- vérifier, par des moyens appropriés et conformes au droit congolais, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré ;
- employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services ;
- utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument ;
- prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données ;
- disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par le présent décret, en particulier pour endosser la responsabilité de dommages, en contractant, notamment, une assurance appropriée ;

- enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice ;
- ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés ;
- avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris les limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et les procédures de réclamation et de règlement des litiges ;
- utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que :

    - seules les personnes autorisées puissent introduire et modifier des données ;
    - l'information puisse être contrôlée quant à son authenticité ;
    - les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et que toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

Article 9 : Les tiers de certification accrédités sont responsables de tout préjudice subi par toute personne qui se serait fixée sur le contenu du certificat qualifié de conformité et délivré par eux.

Article 10 : Le dispositif de création doit garantir la confidentialité des données par les moyens techniques et les procédures appropriés, de façon que :

- les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée ;
- l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne peuvent être trouvées par déduction et que la signature est protégée contre toute falsification par les moyens techniques actuellement disponibles ;
- les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

Seul le titulaire de certificat est responsable de la confidentialité de ces données dès le moment de la création des données afférentes à la création de la signature électronique.

TITRE III : DE L'AGREMENT DES PRESTATAIRES DE SERVICES DE CERTIFICATION ELECTRONIQUE

Article 11 : Les prestataires de service de certification électronique voulant émettre et délivrer les certificats électroniques sécurisés et gérer les services y afférents doivent obtenir un agrément du guichet unique des opérations transfrontalières.

Chapitre 1 : De la composition du dossier d'agrément

Article 12 : Le demandeur de l'agrément dépose, auprès du guichet unique des opérations transfrontalières, un dossier comprenant :

- une fiche de renseignement fournie par le guichet unique des opérations transfrontalières dument remplie et signée par le demandeur de l'autorisation ;
- une lettre de présentation sommaire des activités et services visés. Cette lettre doit clairement préciser la nature du service, les applications souhaitées ;
- une copie de l'immatriculation au registre du commerce et du crédit immobilier ;
- l'identité de la personne physique ou du représentant légal de la personne morale ;
- un casier judiciaire ;
- une déclaration sur l'honneur de la personne physique ou du représentant légal de la personne morale s'engageant à ne pas exercer une autre activité professionnelle ;
- une copie du diplôme, niveau ingénieur en informatique ou réseaux, de la personne considérée comme référent technique du projet ;
- une lettre de proposition d'installation des équipements informatiques concernés fournis par un installateur agrée ;
- une étude financière du projet à réaliser ;
- une description détaillée de tous les registres à tenir et les caractéristiques des dispositifs utilisés pour les gérer ;
- un dossier d'étude technique détaillant notamment :

  - les besoins en termes informatiques ;
  - les caractéristiques techniques des équipements ;
  - les caractéristiques des dispositifs de sécurisation des réseaux utilisés pour la fourniture des services de certification ;
  - le lieu d'implantation ou d'installation des serveurs ;
  - un plan du local du fournisseur et une description des procédures de sécurité adoptées pour la sécurisation du local.

Chapitre 2 : De la procédure de l'agrément

Article 13 : Le guichet unique des opérations transfrontalières délivre un accusé de réception et dispose d'un délai de trente jours pour rendre sa décision.

Article 14 : Le Gouvernement peut, par dérogation, accorder aux personnes morales de droit public, un agrément sur proposition du guichet unique des opérations transfrontalières et sous réserve de l'intérêt du service public (l'armée, la gendarmerie et la police).

TITRE IV : DISPOSITION FINALE

Article 15 : Le présent décret, qui abroge toutes dispositions antérieures contraires, sera enregistré et publié au Journal officiel./-

2014 - 596 Fait à Brazzaville, le 3 novembre 2014

Denis SASSOU-N'GUESSO.-

Par le Président de la République,

Le ministre d'Etat, ministre des transports, de l'aviation civile et de la marine marchande,

Rodolphe ADADA.-

Le ministre d'Etat, garde des sceaux, ministre de la justice et des droits humains,

Aimé Emmanuel YOKA.-

Le ministre d'Etat, ministre de l'économie, des finances, du plan, du portefeuille public et de l'intégration,

Gilbert ONDONGO.-

Le ministre des postes et télécommunications,

Thierry MOUNGALLA.-

La ministre du commerce et des approvisionnements,

Claudine MUNARI.-