JOURNAL OFFICIEL DU SENEGAL

DECRET n° 2008-720 du 30 juin 2008

DECRET n° 2008-720 du 30 juin 2008 relatif à la certification électronique pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

[|RAPPORT DE PRESENTATION|]

Le présent projet de décret est pris en application des dispositions de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.

Le Sénégal a choisi d'adopter le système de la certification comme moyen privilégié d'authentification électronique des personnes et des documents.

L'une des composantes de ce système est la mise en place d'une Autorité de certification.

Le présent décret apporte les précisions relatives, notamment :

1) à la gestion d'un système d'accréditation ;

2) aux conditions de délivrance d'un certificat électronique ;

3) aux obligations de l'autorité et des organismes de certification.

Telle est l'économie du présent projet de décret.

Le Président de la République,

Vu la Constitution, notamment en ses articles 43 et 76 ;

Vu la loi 90-07 du 26 juin 1990 relative à l'organisation et au contrôle des entreprises du secteur parapublic et au contrôle des personnes morales de droit privé bénéficiant du concours financier de la puissance publique ;

Vu la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques :

Vu le décret n° 2004-1038 du 23 juillet 2004 fixant les règles d'organisation et de fonctionnement de l'Agence de l'Informatique de l'Etat (ADIE) ;

Vu le décret 2007-826 du 19 juin 2007 portant nomination du Premier Ministre ;

Vu le décret n° 2008-362 du 7 avril 2008 portant répartition des services de l'Etat et du contrôle des établissements publics, des sociétés nationales et des sociétés à participation publique entre la Présidence de la République, la Primature et les ministères ;

Sur le rapport du Premier Ministre ;

Décrète :

Chapitre premier. - Des conditions générales.

Article premier. - Le présent décret fixe les conditions et les procédures d'exercice de l'activité de certification électronique conformément aux

dispositions de la loi n° 2008-08 du 25 janvier 2008 relatives aux transactions électroniques.

Art. 2. - Au sens du présent décret, on entend par :

1) Certificat : attestation électronique qui lie des données afférentes à la vérification d'une signature ou de tout autre document numérique, à une personne. Le certificat confirmant l'identité d'une personne ou la conformité d'un document, est un lien entre l'entité physique et l'entité électronique.

2) Certification : procédure qui sert à faire valider la conformité d'un système selon certaines normes par un organisme. Elle permet de donner une assurance écrite par l'intervention d'un tiers qu'un produit, un processus ou un service est conforme aux exigences spécifiées.

3) Dispositif de vérification de la signature :

dispositif logiciel ou matériel utilisé pour procéder à la vérification de la signature électronique.

4) Données afférentes à la création de signature :

données que le signataire utilise pour créer une signature électronique ;

5) Dispositif sécurisé de création de signature : dispositif logiciel ou matériel de création de signature qui satisfait aux exigences prévues à l'article 36 du présent décret.

6) Organisme de certification : l'organisme chargé de délivrer les certificats, de leur assigner une date de validité ou de les révoquer.

7) Produit : tout élément matériel ou logiciel destiné à être utilisé pour la fourniture de services de signature électronique notamment pour la création ou la vérification de ladite signature.

8) Signataire : toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une personne physique ou morale qu'elle représente.

9) Titulaire du certificat : une personne, physique ou morale, à laquelle un organisme de certification a délivré une attestation électronique.

Chapitre 2. - De la délivrance des agréments.

Art. 3. - Conformément à l'article 40 de la loi sur les transactions électroniques, l'Agence de l'Informatique de l'Etat (ADIE) est chargée notamment :

1) d'octroyer des agréments aux organismes assurant une activité de certification électronique ;

2) de contrôler le respect par les organismes de certification des dispositions en vigueur en matière de certification ;

3) de contrôler les certificats émis par les organismes de certification de signatures électroniques ;

4) de fixer les caractéristiques du dispositif de création et de vérification de la signature électronique ;

5) de conclure les conventions de reconnaissance mutuelle entre le Sénégal et des pays tiers voire des organisations internationales ;

6) d'émettre, de délivrer et de conserver des certificats électroniques relatifs aux agents de l'Etat ;

7) d'élaborer un cahier des charges, approuvé par décret, qui fixe les conditions et les procédures d'exercice de la politique nationale de certification ;

8) de tenir un registre des organismes de certification agréés.

Art. 4. - Toute personne physique ou morale désirant exercer les activités de fournisseur de services de certification électronique doit obtenir l'autorisation préalable de l'agence de l'informatique de l'Etat.

Les demandes d'agrément sont adressées, soit par lettre recommandée, soit par voie électronique sur le site de l'Agence de l'informatique de l'Etat. Il en est accusé dans les mêmes formes. A défaut, elles peuvent être déposées directement auprès de l'Agence de l'informatique de l'Etat contre décharge.

Art. 5. - Le dossier des demandes d'agrément, leur renouvellement ou leur extension contient obligatoirement les documents suivants :

1) une fiche de renseignement fournie par l'Agence de l'informatique de l'Etat dûment remplie et signée par le demandeur de l'agrément ;

2) les documents justificatifs des moyens matériels, financiers et humains de l'organisme de certification ;

3) les caractéristiques techniques des équipements informatiques à utiliser pour la fourniture des services proposés, accompagnées d'un schéma du dispositif de certification ;

4) une description détaillée des procédures de sécurité adoptées pour la sécurisation des locaux et des équipements informatiques ;

5) un récépissé de paiement des frais de dossier prévu par le cahier des charges mentionné au point 7 de l'article 3 du présent décret.

Art. 6. - L'Agence de l'informatique de l'Etat est tenue de répondre à la demande formulée dans un délai fixé par le cahier des charges prévu au point 7 de l'article 3 du présent décret.

Art. 7. - Les demandes d'agrément sont refusées dans les cas suivants :

1) Si les conditions d'octroi telles que précisées par le cahier des charges ne sont pas respectées ;

2) Si, à l'expiration d'un délai fixé par le cahier des charges susmentionné, le demandeur de l'agrément ne fournit pas à l'Agence de l'informatique de l'Etat les informations nécessaires qu'elle exige pour compléter le dossier.

Art. 8. - Les agréments sont octroyés sur la base d'un rapport de constat établi par les services de l'Agence de l'informatique de l'Etat. Ce rapport comprend une évaluation des moyens techniques, financiers et humains conformément aux dispositions du cahier des charges prévu par le point 7 de l'article 3 du présent décret.

Art. 9. - L'agrément conféré à l'organisme de certification est octroyé à titre personnel. Sa durée est déterminée par le cahier des charges prévu au point 7 de l'article 3 du présent décret. Il ne peut être ni cédé ni transféré à un tiers sans autorisation expresse de l'Agence de l'informatique de l'Etat.

Art. 10. - L'Agence de l'informatique de l'Etat tient un registre des organismes de certification, qui fait l'objet, à la fin de chaque année, d'une publication au Journal officiel.

Cette insertion ne préjudicie en rien la possibilité, pour l'Agence de l'informatique de l'Etat, de publier à tout moment, soit sur son site web, soit dans un ou plusieurs journaux, sénégalais ou étrangers, une radiation du registre des certificats électroniques, si une telle mesure de publicité est commandée par l'intérêt public.

Art. 11. - L'Agence de l'informatique de l'Etat peut, soit d'office, soit à la demande de toute personne intéressée, vérifier ou faire vérifier la conformité des activités d'un organisme de certification délivrant des certificats.

Les opérations de contrôles sont effectuées périodiquement et chaque fois que l'Agence de l'informatique de l'Etat le jugera utile.

Art. 12. - L'Agence de l'informatique de l'Etat peut recourir à des auditeurs externes agréés pour procéder aux vérifications prévues à l'article 11 du présent décret.

Les auditeurs externes doivent justifier d'une qualification professionnelle adéquate, d'une expérience dans le domaine des technologies des signatures électroniques, de la sécurité des systèmes et des réseaux informatiques. Ils doivent également présenter des garanties d'honorabilité professionnelle et d'indépendance par rapport aux organismes de certification dont elles sont appelées à vérifier les activités.

Toute personne désirant être agréée en tant qu'auditeur externe doit en faire la demande écrite auprès de l'Agence de l'informatique de l'Etat, les minima d'expérience, de qualification professionnelle et de formation requis pour l'octroi de l'agrément sont fixés par le cahier des charges prévu à l'article 7 du présent décret.

L'Agence de l'informatique de l'Etat peut conformément au cahier des charges visé à l'alinéa précédent, annuler un agrément en cas de manquement du bénéficiaire à ses obligations ou lorsque les conditions requises pour l'octroi dudit agrément ne sont pas réunies.

Art. 13. - Dans l'accomplissement de leur mission de vérification, les agents de l'Agence de l'informatique de l'Etat, ainsi que les auditeurs externes agréés ont, sur justification de leurs qualités, le droit d'obtenir la communication de toutes les informations ou de tous les documents qu'ils estimeront utiles ou nécessaires à l'accomplissement de leur mission.

Art. 14. - En cas de manquement aux dispositions de la loi sur les transactions électroniques ou celles du présent décret, constaté sur procès verbal par ses agents ou par les auditeurs externes agréés, l'Agence de l'informatique de l'Etat met en demeure l'organisme concerné à se conformer, dans le délai qu'elle détermine, aux dispositions susmentionnées.

Le rapport établi par les personnes mentionnées au présent article est communiqué à l'organisme, de certification qui peut faire valoir ses observations et commentaires.

Si, passé ce délai, l'organisme ne s'est pas conformé aux décisions de l'Agence de l'informatique, la suspension ou le retrait de l'agrément peut être prononcée. Le retrait entraîne automatiquement la radiation de l'organisme de certification.

L'Agence de l'informatique de l'Etat peut également, en cas de refus de la part d'un organisme de certification de collaborer activement lors d'une vérification, procéder à la radiation de l'organisme concerné du registre des certificats électroniques.

Art. 15. - La décision de suspension ou de radiation est notifiée à l'organisme de certification conformément aux dispositions de l'alinéa 2 de l'article 4 du présent décret.

L'organisme de certification est tenu de mentionner immédiatement dans son registre des certificats électroniques la suspension ou la radiation de l'accréditation et d'en informer sans délai les titulaires de certificat.

Art. 16. - En cas de constatation d'une violation grave des dispositions en vigueur en matière de certification, l'Agence de l'informatique de l'Etat peut également en informer les autorités judiciaires compétentes.

Art. 17. -La décision portant sur la suspension ou le retrait de l'agrément est susceptible d'un recours devant les tribunaux compétents.

Chapitre 3. - Des organismes de certification.

Art. 18. - En application de l'article 42 de la loi sur les transactions électroniques, l'organisme de certification, agréé conformément à l'article 40 de la loi susvisée, délivre un certificat, après avoir vérifié les conditions définies à l'article 33 du présent décret.

L'organisme de certification peut délivrer un ou plusieurs certificats à toute personne qui en fait la demande conformément aux textes en vigueur.

Art. 19. - Tout organisme de certification doit :

1) informer les utilisateurs des certificats de leurs droits et leurs obligations ;

2) veiller à ce que la date, l'heure d'émission et de révocation du certificat soient mentionnées clairement ;

3) assurer la gestion d'un registre des certificats électroniques rapide et sécurisé ainsi qu'un service de révocation immédiat ;

4) mettre en place une politique de sécurité adéquate pour ses équipements terminaux ainsi que pour ses serveurs dont l'accès est contrôlé ;

5) vérifier, sur présentation d'un document officiel d'identification, l'identité et, le cas échéant, les qualités spécifiques de la personne physique ou morale à laquelle un certificat est délivré. Cette vérification peut s'effectuer par voie électronique ;

6) avoir du personnel ayant des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées ;

7) faire la preuve qu'il est suffisamment fiable pour fournir des services de certification ;

8) utiliser des systèmes et des produits fiables qui sont protégés contre les modifications éventuelles et qui assurent la sécurité technique des fonctions qu'ils assument :

9) prendre des mesures contre la contrefaçon des certificats ;

10) garantir, lorsqu'il génère des données afférentes à la création de signature, la confidentialité au cours du processus de génération de ces données ;

11) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle l'organisme de certification a fourni des services de gestion de clés ;

12) Elaborer, mettre en œuvre et publier les modalités de l'utilisation en bonne et due forme des certificats ;

13) Utiliser des systèmes fiables pour stocker les certificats de telle sorte :

a) que l'information puisse être contrôlée quant à son authenticité ;

b) que seules les personnes autorisées puissent introduire et modifier des données ;

c) qu'ils ne soient disponibles au public uniquement que pour des recherches avec le consentement du titulaire dudit certificat.

Art. 20. - Tout organisme de certification doit procurer, sur un support durable et de manière intélligible, les informations nécessaires à l'utilisation correcte et sûre de ses services, notamment :

1) la procédure à suivre afin de créer et de vérifier une signature électronique ;

2) les conditions contractuelles de délivrance d'un certificat ;

3) les tarifs appliqués aux services fournis ;

4) les obligations qui pèsent sur le titulaire du certificat et l'organisme de certification ;

5) les modalités et les conditions précises d'utilisation des certificats, y compris les limites imposées à leur utilisation ;

6) les procédures de réclamation et de règlement des lignes.

Ces informations doivent être approuvées, au préalable, par l'Agence de l'informatique du Sénégal.

Art. 21. - Un certificat non révoqué est renouvelé sur demande à l'approche de la fin de la validité dudit certificat.

Art. 22. - L'organisme de certification révoque un certificat immédiatement lorsque :

1) la date de validité expire ;

2) la demande émane de son titulaire ;

3) le certificat a été délivré sur la base d'informations erronées ou falsifiées ;

4) les informations contenues dans le certificat ne sont plus conformes à la réalité ;

5) la confidentialité des données à caractère personnel du certificat a été violée ;

6) le certificat a été utilisé frauduleusement ;

7) le titulaire décède ou en cas de dissolution de la personne morale.

Art. 23. - En cas de révocation, l'organisme de certification informe le titulaire du certificat dans les meilleurs délais en motivant sa décision.

Lorsque la révocation intervient suite à l'expiration de la date de validité, l'organisme de certification doit prévenir le titulaire de l'échéance du certificat. Le délai d'avertissement est fixé par le cahier des charges prévu au point 7 de l'article 3 du présent décret.

La révocation d'un certificat est définitive.

Art. 24. - L'organisme de certification doit inscrire impérativement, sans délai, la décision de révocation dans le registre des certificats électroniques prévu au point 3 de l'article 19 du présent décret.

La révocation devient opposable aux tiers dès son inscription dans ledit registre.

Art. 25. - L'organisme de certification qui délivré à l'intention du public un certificat ou qui le garantit est responsable du préjudice causé à toute personne qui se fie raisonablement :

1) à l'exactitude des informations contenues dans le certificat délivré ;

2) à l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat détenait les données afférentes à la création de ladite signature ;

3) à l'assurance que le dispositif de création de signature et le dispositif de vérification de signature fonctionnent ensemble de façon complémentaire, au cas où le prestataire a généré les deux dispositifs.

Art. 26. - Le registre des certificats éléctroniques, mentionné au point 3 de l'article 19 du présent décret, contient le nom et la qualité des demandeurs.

Si le demandeur est une personne morale, il est fait mention du nom et de la qualité de la personne physique qui représente ladite pesrsonne et qui fait usage de la signature liée au certificat.

La non inscription d'uné révocation d'un certificat dans le registre des certificats électroniques engage la responsabilité de l'organisme de certification.

Art. 27. - L'orsqu'un certificat arrive à échéance ou a été révoqué, son titulaire ne peut plus utiliser les données correspondantes.

L'organisme de certification n'est pas tenu responsable des préjudices dont pourraient être victimes les utilisateurs du certificat révoqué ou qui est à son terme.

De même, il n'est pas responsable du préjudice résultant de l'usage abusif d'un certificat.

Art. 28. - En cas de cessation d'activités, l'organisme de certification accrédité informe dans un délai d'un mois l'Agence de l'informatique de l'Etat de son intention de mettre fin à ses activités ou, le cas échéant, de son incapacité de les poursuivres.

Dans cette hypothèse, l'organisme de certification indique, à chaque titulaire de certificat, le droit qu'il a d'accepter ou de refuser le transfert envisagé ainsi que les délais et modalités dans lesquelles il peut donner ou refuser son accord. Au terme du délai imparti, le certificat est réputé nul et nul effet à défaut d'acceptation écrite de son titulaire.

Le transfert des certificats est opéré aux conditions suivantes :

1) l'organisme de certification avertit chaque titulaire de certificat encore en vigueur qu'il envisage de transférer les certificats à un autre organisme de certification au moins un mois avant le transfert envisagé ;

2) l'organisme de certification indique à chaque titulaire de certificat leur faculté de refuser le transfert envisagé ainsi que les délais et modalités dans lesquelles il peut le refuser. A défaut d'acceptation expresse du titulaire au terme de ce délai, le certificat est révoqué d'office.

Art. 29. - Le décès, l'incapacité, la fallite, la dissolution volontaire et la liquidation, ou tout autre motif involontaire d'arrêt des activités sont assimilés à une cessation d'activité de l'organisme de certification.

Art. 30. - L'organisme de certification ne peut tranférer ou déplacer, à l'étranger, ses serveurs contenant des données afférentes aux certificats délivrés, sans l'accord de l'Agence de l'informatique de l'Etat.

Art. 31. - L'organisation de certification doit conserver, conformément à l'article 37 de la loi sur les transactions électroniques et à compter de la date de son traitement, les enregistrements relatifs, notamment à :

1) l'émission, le renouvellement, la suspension et la révocation des certificats ;

2) les procédures de gestion des équipements et des programmes informatiques ;

3) tout document dont la conservation est jugée utile par l'Agence de l'informatique de l'Etat.

Chapitre 4. - Des certificats.

Art. 32. - Les certificats que l'organisme de certification peut émettre sont classés en plusieurs catégories, notamment :

1) les certificats de classe 1 : aucun contrôle de l'identité du détenteur du certificat n'est requis ;

2) les certificats de classe 2 : l'organisme de certification effectue un contrôle sur le dossier de demande de certificat ;

3) les certificats de classe 3 : l'organisme de certification demande une vérification physique avec la présence de l'utilisateur ;

4) les certificats de classe 4 : l'organisme de certification exige la présence de l'utilisateur qui recevra son certificat sur un support physique (carte à puce ou clé USB).

L'Agence de l'informatique de l'Etat peut décider, en cas de besoin, de créer d'autres catégories de certificats électroniques.

Art. 33. - Tout certificat doit contenir les informations suivantes :

1) l'identification de l'organisme de certification ;

2) le nom du demandeur ou de son pseudonyme ;

3) les données afférentes à la vérification de la signature ;
4) la période de validité du certificat ;

5) le code d'identification du certificat ;

6) la qualité du demandeur du certificat ;

7) l'accréditation de l'organisme de certification ;

8) les limites à l'utilisation du certificat.

En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de la conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer immédiatement le certificat.

Art. 34. - Toute publication d'un certificat électronique est soumise au consentement de son titulaire.

Art. 35. - Les certificats électroniques, délivrés par un organisme de certification établi dans un pays tiers, ont la même valeur juridique au Sénégal que ceux délivrés par l'Agence de l'informatique de l'Etat, à condition que :

1) l'organisme de certification respecte la légistation sénégalaise en vigueur en la matière ;

2) le certificat ou l'organisme de certification soit reconnu dans le cadre d'un accord bilatéral ou multilatéral entre le Sénégal et des pays tiers ou des organisations internationales.

L'agence de l'informatique de l'Etat publie la liste des accords conclus.

Chapitre 5. - De la signature électronique.

Les dispositifs sécurisés de création de signature électronique doivent garantir, par des moyens techniques et des procédures appropriés, que :

1) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit assurée ;

2) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction ;

3) la signature créée soit protégée contre toute falsification par les moyens techniques appropriés et évolutifs ;

4) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par des tiers.

Art. 37. - Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

Art. 38. - En application de l'article 41 de la loi sur les transactions électroniques, la signature nécessaire à la perfection d'un acte sous seing privé peut être manuscrite ou électronique.

Art. 39. - La signature électronique consiste en un ensemble de données qui doivent :

1) permettre d'identifier le signataire ;

2) être liées uniquement au signataire ;

3) être créées par des moyens que le signataire puisse garder sous son contrôle exclusif ;

4) reposer sur un certificat électronique.

Chapitre 6. - Dispositions communes.

Art. 40. - L'Agence de l'informatique de l'Etat et les organismes de certification sont tenus au respect des dispositions légales régissant le traitement de données à caractère personnel.

Toutefois, lorsque le titulaire du certificat utilise un pseudonyme, l'organisme de certification ayant délivré le certificat est tenu de communiquer toute donnée relative à l'identité du titulaire aux autorités judiciaires compétentes.

Art. 41. - Les personnes exerçant ou ayant exercé une activité, soit pour l'Agence informatique de l'Etat agissant en tant qu'autorité d'accréditation, soit pour l'organisme de certification, sont tenus au secrét professionnel et sont passibles des peines prévues par le Code pénal.

Art. 42. - Le Premier Ministre et les ministres sont chargé de l'application du présent décret qui sera publié au Journal officiel.

Fait à Dakar, le 30 juin 2008.

[/Abdoulaye WADE.

Par le Président de la République :

Le Premier Ministre,

Cheikh Hadjibou SOUMARE./]