Arrêté du ministre de l'industrie, du commerce et des nouvelles technologies n°154-10 du 5 rabii II 1431 fixant la forme de la demande d'agrément de prestataire de services de certification électronique et portant approbation du modèle de cahier des charges l'accompagnant. (B.O. n°5830 du 15 avril 2010).

Vu le décret n°2-08-518 du 25 joumada I 1430 (21 m ai 2009) pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi n° 53-05 relative à l'échange électronique des données juridiques, notamment ses articles 21 et 22 ;

Sur proposition de l'Agence nationale de réglementation des télécommunications,

Article premier : La demande d'agrément de prestataire de services de certification électronique en vue d'émettre et de délivrer des certificats électroniques sécurisés et de gérer les services y afférents, visée à l'article 21 du décret susvisé n°2-08-518 du 25 joumada I 1430 (21 mai 2009), doit être établie conformément au modèle annexé au présent arrêté.

Article 2 : Est approuvé, tel qu'annexé au présent arrêté, le modèle du cahier des charges devant accompagner la demande visée à l'article premier ci-dessus.

Article 3 : Le présent arrêté sera publié au *Bulletin officiel*.

Modèle de la demande d'agrément de prestataire de services de certification électronique

I. Nature de la demande :

- Premier agrément
- Renouvellement de l'agrément

II. Identification du demandeur :

Raison sociale	.....
Forme de la société	.....
Inscription au registre de commerce	N°: ..... Ville : .....
N°CNSS	.....
N°de la Patente	.....
Siège social	.....
Téléphone	.....
Fax	.....
Courriel	.....
Site Web	.....

III. Identification de la personne chargée du dossier administratif :

Prénom, Nom	.....
Qualité	.....
Nationalité	.....
Pièce d'identité	Nature : .....N°: .....

	Validité : ..... Lieu de délivrance : .....
Adresse	.....
Téléphone	.....
Fax	.....
Courriel	.....

IV. - Les noms et qualités des dirigeants de la société et des membres de son conseil d'administration

(Joindre les listes correspondantes et les documents habilitant les personnes devant agir au nom de la société)

V. - Les états financiers des trois derniers exercices et/ou toutes pièces justifiant les capacités financières de l'organisme

(Joindre les pièces correspondantes)

VI. - Les statuts de la société, son règlement intérieur ou tout autre texte régissant son fonctionnement

(Joindre les pièces correspondantes)

Fait à ....., le ..... (.....)....
Signature et cachet

*** * ***

Modèle du cahier des charges devant accompagner la demande d'agrément de prestataire de services de certification électronique

Chapitre premier : Dispositions Générales

Article premier : Le présent cahier des charges a pour objet de fixer les prescriptions que doit observer ..... (indiquer les éléments d'identification du demandeur) ....., ci-après désigné «prestataire», pour émettre et délivrer des certificats électroniques sécurisés et gérer les services y afférents.

Article 2 : Le présent cahier des charges entre en vigueur à compter de la date indiquée par l'agrément délivré au prestataire. Il est valable pour la durée de validité dudit agrément.

Article 3 : Le présent cahier des charges est modifié lorsque l'un des éléments sur la base duquel l'agrément a été délivré au prestataire a subi une modification.

Article 4 : Le prestataire doit :

- se conformer aux conditions prévues par l'agrément qui lui a été délivré et ce, durant toute la période de validité dudit agrément ;

- informer l'autorité gouvernementale chargée des nouvelles des technologies, dans un délai maximum de deux (2) mois, de sa volonté de mettre fin à ses activités, en application des dispositions de l'article 23 de la loi n°53 -05 relative à l'échange électronique des données juridiques ;

- informer, sans délai, l'Agence nationale de réglementation des télécommunications, ci-après désignée «ANRT», de l'arrêt de ses activités en cas de liquidation judiciaire, en application des dispositions de l'alinéa 3 de l'article 23 de la loi précitée n°53-05 ;

- permettre aux agents de l'ANRT, ainsi qu'aux experts désignés par elle, d'accéder à tout établissement et de prendre connaissance de tous mécanismes et moyens techniques relatifs aux services de certification électronique sécurisée qu'ils estimeront utiles ou nécessaires à l'accomplissement de leur mission, en application des dispositions de l'article 19 de la loi précitée n°53-05 ;

- permettre aux agents de l'ANRT habilités à cet effet et assermentés de rechercher et de constater, par procès-verbal, les infractions aux dispositions de la loi précitée n° 53-05 et des textes pris pour son application, d'accéder aux locaux, terrains ou moyens de transport à usage professionnel, de demander la communication de tous documents professionnels et en prendre copie et de recueillir, sur convocation ou sur place, les renseignements et justifications, en application des dispositions de l'article 41 de la loi précitée n°53-05.

Chapitre 2 : Informations relatives au personnel du prestataire

Article 5 : Les copies des pièces d'identité, des titres et diplômes du personnel chargé de la certification électronique, ainsi que la description des qualifications, dont ce personnel dispose en la matière, et les fonctions qu'il occupe, accompagnée d'un document justifiant desdites qualifications sont jointes à l'annexe A au présent cahier des charges intitulée : «identité et compétences du personnel du prestataire».

Chapitre 3 : Conditions administratives et techniques garantissant le respect des obligations du prestataire

Section 1 : Conditions administratives

Article 6 : Le prestataire doit communiquer à l'ANRT les documents suivants :

* le certificat électronique dont il dispose et qui contient la clé publique correspondant à la clé privée qu'il utilise pour signer les certificats électroniques émis par ses soins ;

* la «Déclaration des Pratiques de Certification» correspondant à ses activités de certification électronique ;

* la notification relative à la révocation du certificat électronique dont il dispose ou tout événement ayant affecté la fiabilité dudit certificat ;

* la notification de tout changement apporté aux documents intitulés «Politique de Certification» et «Déclaration des pratiques de certification» avant la mise en oeuvre dudit changement ;

* copie des polices d'assurance souscrites par lui pour couvrir ses responsabilités civile et professionnelle des risques encourus dans le cadre de l'exercice de ses activités ;

* copie du récépissé attestant le dépôt d'une déclaration préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie ;

* copie de l'autorisation préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie, délivrée, s'il y a lieu, par l'autorité gouvernementale chargée des nouvelles technologies.

Section 2 : Conditions techniques

Article 7 : Les spécifications techniques et les standards applicables pour la fourniture de services relatifs à l'exercice des activités de prestataire de services de certification électronique sont comme suit :

a) ETSI TS 101 456 - (Policy requirements for certification authorities issuing qualified certificates) ou sa traduction française AFNOR Z74 400 - (Exigences concernant la politique mise en oeuvre par les autorités de certification délivrant des certificats qualifiés) ;

b) IETF RFC 3647 - (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) à

laquelle doit se conformer le prestataire tout en se basant sur la «politique de certification de référence» «PC-type», téléchargeable sur le site de l'ANRT : ;

c) Infrastructures à clés publiques telles que précisées dans la recommandation UIT-T X.509 (Technologies de l'information - Interconnexion des systèmes ouverts - L'annuaire : cadre général des certificats de clé publique et d'attribut) ;

d) le format d'un certificat électronique est celui de la norme ISO/IEC 9594-8 ou recommandation UIT-T X.509 v3 ;

e) Algorithmes à clés publiques tels que décrits dans le standard IEEE P 1363 - Standard Specifications For Public Key Cryptography, pour un système appartenant aux trois familles d'algorithmes de cryptographie asymétrique :

* Logarithme discret : Diffie-Hellman, Menezes-Qu-Vanstone (MQV), DSA avec SHA-1 ou version évoluée, Nyberg-Rueppel ;

* Factorisation des grands entiers : RSA tel que décrit dans ANSI X9.31, RSA Encryption, Rabin-Williams ;

* Courbes elliptiques : ECDSA (Elliptic-Curve DSA) ;

f) Standards pour la cryptographie à clé publique :

RSA PKCS (Public Key Cryptography Standard) :

* PKCS#1 RSA Cryptography Standard (1024, 2048 bit) ;
* PKCS#3 Diffie-Hellman Key Agreement Standard ;
* PKCS#5 Password Based Cryptography Standard ;
* PKCS#6 Extended-Certificate Syntax Standard ;
* PKCS#7 Cryptographic Message Syntax standard ;
* PKCS#8 Private Key Information Syntax standard ;
* PKCS#9 Selected Attribute Types ;
* PKCS#10 Certification Request Syntax standard ;
* PKCS#11 Cryptographic Token Interface Standard ;
* PKCS#12 Personal Information Exchange Syntax standard ;
* PKCS#13 : Elliptic Curve Cryptography Standard ;
* PKCS#15 Cryptographic Token Information Format Standard ;

g) Recommandations FIPS (Federal Information Processing Standard) :

* FIPS 180-3, Secure Hash Standard ;

* FIPS 186-3, Digital Signature Standard ;

* FIPS 140-2, Security requirements for Cryptographic Modules (niveau 3) pour la sauvegarde de la clé privée du prestataire ;

* FIPS 198-1, the Keyed-Hash Message Authentication Code (HMAC) ;

* FIPS 197, Advanced Encryption Standard ;

h) Syntaxe standard pour le certificat électronique :

Les certificats délivrés par le prestataire doivent se conformer au format du standard de l'UIT X.509 v3 ;

k) Syntaxe standard pour la liste des certificats révoqués :

Les certificats délivrés par le prestataire doivent se conformer au format du standard de l'UIT X.509 v2 ;

i) Standard pour la fourniture de service d'horodatage :

* La fourniture de services d'horodatage doit être conforme à la référence IETF RFC 3161 : Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

Le prestataire doit indiquer, dans une annexe B jointe au présent cahier des charges, intitulée : «conditions techniques», les modalités selon lesquelles il entend appliquer les spécifications techniques et les standards susmentionnés.

Chapitre 4 : Enumération des moyens ou des prestations de cryptographie

Article 8 : Les moyens ou les prestations de cryptographie que le prestataire peut fournir, utiliser ou exploiter sont énumérés à l'annexe C jointe au présent cahier des charges, intitulée : «Moyens ou prestations de cryptographie».

Chapitre 5 : Caractéristiques techniques des équipements et des dispositifs utilisés pour la fourniture des services

Article 9 : Les caractéristiques techniques des équipements et des dispositifs à utiliser par le prestataire pour la fourniture des services sont décrites à l'annexe D jointe au présent cahier des charges, intitulée : «Caractéristiques techniques des équipements et des dispositifs utilisés».

Chapitre 6 : Description des procédures et des moyens mis en oeuvre pour émettre des certificats électroniques

Article 10 : Le prestataire doit :

a) ajuster ses opérations et son fonctionnement pour permettre l'émission des certificats électroniques sécurisés ;

b) porter à la connaissance des personnes auxquelles il délivre des certificats électroniques les montants de l'assurance souscrite couvrant les dommages résultant de sa faute professionnelle ;

c) respecter et contrôler les mesures de sécurité concernant aussi bien la sécurité relative au personnel employé dans la fourniture des services de certification électronique que les mesures prises en cas de gestion d'incidents et ce, afin de prévenir les fraudes et les failles de sécurité.

A cet effet, il prépare et tient à jour des manuels détaillés décrivant les procédures à suivre et énumérant les moyens à mettre en oeuvre pour toutes ses activités. Ces manuels doivent être communiqués à l'ANRT, à sa demande.

En outre, il met en place un système de contrôle d'accès et d'intégrité, en particulier des détecteurs d'intrusions, de recherche de virus, de prévention des attaques par déni de service et des mesures de sécurité physique pour les systèmes de sauvegarde et de traitement des informations fournies par les clients.

Article 11 : Le prestataire doit garder des enregistrements de toutes ses activités et s'assurer de leur mise à jour afin de détecter toute anomalie de son système.

Chapitre 7 : Conditions techniques et organisationnelles de gestion des certificats électroniques sécurisés

Article 12 : Le prestataire doit :

* s'assurer de l'intégrité des certificats électroniques sécurisés qu'il émet, en utilisant les spécifications techniques et les standards visés à l'article 7 ci-dessus et ce, lors de l'enregistrement, de la génération, de la création, de la publication, du renouvellement, de la suspension, de la révocation et de l'archivage desdits certificats ;

* s'assurer que les personnes auxquelles un certificat électronique est délivré peuvent vérifier ledit certificat ;

* conserver les données afférentes à la création des certificats électroniques révoqués et les listes desdits certificats, de

manière à permettre la fourniture des éléments de preuve pour les différents types d'actes traités, en application de la loi précitée n°53-05 et des textes pris pour son appli cation. Toutefois, le prestataire ne doit pas conserver les données afférentes à la création de signature électronique des personnes auxquelles il fournit le service.

Les conditions techniques et organisationnelles de gestion des certificats électroniques sécurisés sont décrites, de manière exhaustive, par le prestataire dans un document intitulé : «Politique de Certification» joint à l'annexe E au présent cahier des charges, conformément aux prescriptions de la «Politique de certification de référence», visée à l'article 7 ci-dessus.

Chapitre 8 : Eléments de vérification de la validité des certificats électroniques

Article 13 : Les éléments techniques nécessaires à la vérification de la validité des certificats électroniques sont décrits par le prestataire, de manière exhaustive, à l'annexe F jointe au présent cahier des charges, intitulée : «Eléments de vérification de la validité des certificats électroniques».

Chapitre 9 : Moyens ou prestations de cryptographie

Article 14 : Les moyens ou les prestations de cryptographie dont le prestataire agréé est autorisé à gérer les conventions secrètes figurent à l'annexe G jointe au présent cahier des charges intitulée : «Moyens ou prestations de cryptographie».

Chapitre 10 : Conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations de cryptographie

Article 15 : Les conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations de cryptographie et les mesures nécessaires pour assurer leur intégrité et leur sécurité sont décrites à l'annexe H jointe au présent cahier des charges, intitulée : «Conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations de cryptographie».

Chapitre 11 : Conditions applicables aux conventions secrètes en cas de cessation d'activité ou de retrait de l'agrément

Article 16 : Le format électronique standardisé dans lequel doivent être transcrites les conventions secrètes, en cas de cessation d'activité ou de retrait de l'agrément est indiqué à l'annexe I-1 jointe au présent cahier des charges, intitulée : «Format électronique standardisé de transcription des conventions secrètes».

Article 17 : Les conditions dans lesquelles sont remises à un autre organisme agréé les conventions secrètes de cryptographie, en cas de cessation d'activité ou à la demande de l'utilisateur, sont indiquées à l'annexe I-2 jointe au présent cahier des charges, intitulée : « Conditions de remise à un autre organisme agréé des conventions secrètes ».

Chapitre 12 : Conditions applicables aux certificats électroniques sécurisés en cas de cessation d'activité ou de retrait de l'agrément

Article 18 : En cas de retrait de l'agrément conformément aux dispositions de l'article 39 de la loi précitée n°53-05, les conditions dans lesquelles la gestion des certificats électroniques sécurisés et les services y afférents est confiée à un autre prestataire de services de certification électronique agréé sont indiquées à l'annexe J-1 jointe au présent cahier des charges, intitulée : « Conditions de transfert à un autre prestataire de la gestion des certificats électroniques sécurisés ».

Article 19 : En cas de retrait de l'agrément conformément aux dispositions de l'article 39 de la loi précitée n°53-05, les conditions dans lesquelles les titulaires des certificats électroniques sécurisés sont avertis du transfert de la gestion desdits certificats ou de leur révocation sont indiquées à l'annexe J-2 jointe au présent cahier des charges, intitulée : « Conditions d'information des titulaires du transfert ou de la révocation de leurs certificats sécurisés ».