REPUBLIQUE DU SENEGAL

PRESIDENCE DE L A REPUBLIQUE

SECRETARIAT GENERAL

Commission nationale de Cryptologie

MODELE DU CAHIER DES CHARGES

DEVANT ACCOMPAGNER

LA DEMANDE D'AGREMENT DE PRESTATAIRE DE CRYPTOLOGIE

Article premier : Définitions

Dans le présent cahier des charges, il est fait usage de termes entendus dans la manière suivante :

- **« le prestataire » ou « le gestionnaire »** : l'organisme agréé auquel est confiée la gestion, pour le compte d'autrui, des conventions secrètes de cryptologie permettant d'assurer des fonctions de confidentialité, au sens du 15. de l'article 3 de la loi 2008-41 du 20 aout 2008 sur la Cryptologie au Sénégal;
- **« le client »** ou **« l'utilisateur »** : personne morale ou physique ayant passé un contrat avec le prestataire ou le gestionnaire;
- **« la gestion des conventions secrètes »** : prestation consistant en la détention, la certification, la distribution ainsi que, éventuellement, la génération des clefs dans des conditions définies au présent cahier des charges;
- **« la remise des conventions sécrètes »** : opération de délivrance des conventions secrètes d'un utilisateur à une autorité habilitée qui le requiert;
- **« la mise en œuvre des conventions secrètes »** : opération de restitution des données claires d'un utilisateur, effectuée à la demande d'une autorité habilitée après fourniture par cette autorité des données chiffrées.

CHAPITRE PREMIER : DISPOSITIONS GENERALES

Article 2 :

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 fournir des prestations de cryptologie soumises à autorisation.

Article 3 :

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 quatre (4) ans conformément au décret.

Article 4 :

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

Article 5 :

Le prestataire doit :

- se conformer aux conditions prévues par la loi 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal et ses décrets d'application n°2010-1209 du 13 septembre 2010 et n°2012-1508 du 31 décembre 2012, durant toute la période de validité dudit agrément.

- se soumettre régulièrement aux vérifications et contrôles décidées par les autorités administratives et judiciaires compétentes. A cet effet, il permet aux agents ou experts commissionnés l'accès aux locaux et installations et leur communique tous les documents professionnels nécessaires pour effectuer les vérifications et les contrôles.

CHAPITRE 2 : INFORMATIONS RELATIVES AU PERSONNEL DU PRESTATAIRE

Article 6 :

Les copies des pièces d'identité, des titres et diplômes du personnel chargé de la fourniture des prestations de cryptologie, 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 en annexe au présent cahier des charges intitulé.

Le prestataire s'engage à porter à la connaissance de tous les membres de son personnel, concernés par la prestation, les obligations liées à la gestion des conventions secrètes de cryptologie et des peines encourues au titre des dispositions du code pénal.

Le prestataire s'engage à faire signer à ses personnels mentionnés un document où il reconnait avoir pris connaissance de la politique de sécurité de l'organisme et de leurs responsabilités en cas de manquement à leur obligation.

Ces personnels font l'objet d'une habilitation par la Commission Nationale de Cryptologie, en application de l'article 48 du décret 2010-1209 du 13 septembre 2010.

CHAPITRE 3 : CONDITIONS ADMINISTRATIVES ET TECHNIQUES GARANTISSANT LE RESPECT DES OBLIGATIONS DU PRESTATAIRE

Section première : Conditions administratives

Article 7 :

Le prestataire doit communiquer au Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information les documents suivants :

- Copie des contrats qu'il a conclus avec le client pour la gestion de ses conventions secrètes. Ces contrats doivent obligatoirement comprendre :
    - les références de l'agrément, sa durée de validité et sa date d'expiration, ainsi que tout élément d'information que le présent cahier des charges impose de communiquer aux utilisateurs ;
    - des clauses relatives à la sécurité des conventions secrètes que le prestataire gère pour le compte du client ;
    - les modalités selon lesquelles le client ou toute autre personne mandatée par lui à cet effet pourra se faire délivrer copie de ses conventions secrètes durant la durée de validité de son contrat avec l'organisme agréé ou après la fin dudit contrat ;
- copie des polices d'assurance souscrites par lui pour couvrir ses responsabilités civile et professionnelle contre les risques encourus dans le cadre de l'exercice de ses activités ;
- la liste de ses clients indiquant leur identité et la nature de la prestation actualisée à la suite de toute modification.

Tout changement concernant le personnel, les locaux, les prestations fournies, les procédures et les moyens relatifs à la fourniture desdites prestations doit être communiqué, sans délai, au Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information.

Section 2 : **Conditions techniques**

Article 8 :

Le prestataire doit respecter et contrôler les mesures de sécurité qu'il met en place pour le bon fonctionnement de ses activités et notamment celles qui concernent la sécurité relative au personnel employé dans la fourniture des prestations de cryptologie, aux équipements, aux informations et aux locaux utilisés, ainsi que les mesures prises en cas de gestion d'incidents en vue de prévenir les fraudes et les failles de sécurité.

- ..... *(indiquer ou joindre en annexe, le cas échéant, le schéma de contrôle des mesures de sécurité ou le protocole proposé à cet effet)* .....

Article 9 :

Le module cryptographique permettant de procéder à la génération et la gestion des conventions secrètes doit répondre aux exigences de sécurité suivantes :

- garantir la robustesse cryptographique des conventions secrètes générées ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des conventions secrètes qui ne sont plus utilisées ;
- garantir la confidentialité et l'intégrité des conventions secrètes ;
- assurer l'accès aux conventions secrètes exclusivement aux utilisateurs autorisés et protéger lesdites conventions contre toute utilisation par des tiers.

Article 10 :

Le module cryptographique permettant le chiffrement des données à protéger doit répondre aux exigences de sécurité suivantes :

- garantir la confidentialité et l'intégrité des données à chiffrer ;
- assurer l'accès aux conventions secrètes exclusivement aux utilisateurs autorisés et protéger lesdites conventions contre toute utilisation par des tiers.

Article 11 :

Le module de déchiffrement, permettant de procéder au déchiffrement des données qui ont été protégées en intégrité et en confidentialité avec des conventions secrètes, doit répondre aux exigences de sécurité suivantes :

- détecter les défauts d'intégrité des données restituées ;
- assurer l'accès aux conventions secrètes exclusivement aux utilisateurs autorisés et protéger lesdites conventions contre toute utilisation par des tiers.

Chapitre 4 : Enumération des moyens ou prestations de cryptographie, proposés aux clients

Article 12 :

Le prestataire s'engage à ne fournir à ses clients des conventions secrètes que pour les seuls moyens ou les prestations de cryptographie énumérées ci-dessous :

(*à compléter par le gestionnaire, en précisant pour chaque moyen ou prestation :*

- *le nom du moyen ou prestation*
- *le nom ou la dénomination sociale du fournisseur*
- *le numéro d'autorisation de fourniture ou le numéro du récépissé de déclaration délivré par la Commission nationale de Cryptologie.)*

Chapitre 5 : Enumération des moyens de cryptographie utilisés ou exploités par le prestataire

Article 13 :

Le prestataire utilise ou exploite, pour la fourniture de ses prestations de cryptographie visées à l'article 12 ci-dessus, les moyens de cryptographie ci-après listés en précisant pour chaque moyen:

(*à compléter par le prestataire, en précisant pour chaque moyen ou prestation :*

- *le nom du moyen ou prestation*
- *le nom ou la dénomination sociale du fournisseur*
- *le numéro d'autorisation de fourniture ou le numéro du récépissé de déclaration délivré par la Commission nationale de Cryptologie.)*

Chapitre 6 : description des procédures et moyens mis en œuvre pour la fourniture des prestations

Article 14 :

Pour fournir les prestations visées à l'article 12 ci-dessus, le prestataire suit les procédures suivantes :

- ..... *(description des procédures)* .....

Article 15 :

Pour fournir les prestations visées à l'article 11 ci-dessus, les moyens mis en œuvre par le prestataire sont les suivants :

- ..... *(indiquer, pour chaque prestation, la nature de celle-ci et les moyens utilisés)* .....

Article 16 : Lieu de remise des conventions secrètes

A compléter par le prestataire si le lieu est différent du lieu de gestion et de celui de remise des conventions secrètes)

Chapitre 7 : Caractéristiques techniques des équipements et des dispositifs utilisés pour la fourniture des prestations

Article 17 :

Les caractéristiques techniques des équipements et des dispositifs utilisés pour la fourniture des prestations de cryptographie sont les suivantes :

- ..... *(indiquer pour chaque prestation la nature de celle-ci et les caractéristiques techniques des équipements et des dispositifs correspondants utilisés ou, le cas échéant, renvoyer à une annexe)*.....)

Chapitre 8 : Conditions de mise en œuvre ou de remise des conventions secrètes

Article 18 :

Le prestataire s'engage à prévoir et à communiquer au Service Technique Central des Chiffres et de la Sécurité des Systèmes d'informations les procédures qui permettent, le cas échéant, la mise en œuvre ou la remise des conventions secrètes.

Article 19 : moyens de cryptologie utilisés pour la mise en œuvre des clefs

Le gestionnaire détient et utilise aux fins exclusives de mise en œuvre au profit des autorités administratives ou judiciaires compétentes les moyens ci-dessous énumérés

(*à compléter par le prestataire, en précisant pour chaque moyen ou prestation :*
- *le nom du moyen ou prestation*
- *le nom ou la dénomination sociale du fournisseur.)*

Article 20 : lieu de remise des conventions secrètes

Le gestionnaire s'engage à maintenir un service permanent de remise des conventions secrètes dans les locaux suivants :

(A compléter par le prestataire si le lieu est différent du lieu de gestion des conventions secrètes)

Article 21 : Registre des demandes de remise ou de mise en œuvre des conventions secrètes

Le prestataire tiendra un registre pour les demandes effectuées par les autorités administratives et judiciaires compétentes.

Article 22 : Cessation d'activité

En cas de cessation d'activités ou de retrait d'agrément ou à la demande du client, le prestataire s'engage à:

- communiquer à ses clients la liste des organismes agréés offrant les mêmes services et les mêmes garanties ;
- confier, sur un support électronique standardisé, au prestataire désigné, en application de l'article 67 du décret 2010-1209 du 13 septembre 2010, les conventions secrètes qu'il détenait sous le format électronique standard international ASN. 1 (*Abstact Syntax Notation*) ;
- informer les clients de la remise de leurs conventions secrètes au prestataire désigné.

Chapitre 9 : Conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations de cryptographie et mesures prises pour assurer leur intégrité et leur sécurité

Article 23 : Sécurité des locaux

Le prestataire s'engage à effectuer la gestion des conventions secrètes, objet de l'agrément, dans les locaux suivants :

- ..... *(indiquer le ou les locaux affectés à chaque type d'activité)* .....

Ces locaux doivent être aménagés de façon à assurer la sécurité des conventions secrètes suivant les prescriptions ci-après :

- disposer d'au moins une zone à accès contrôlé, contre toute intrusion extérieure, pour abriter les activités de gestion, de mise en œuvre ou de remise des conventions secrètes. L'accès à cette zone est contrôlé par tout moyen physique et enregistré. Le personnel autorisé à y accéder est limité au strict besoin du bon fonctionnement du service et figure sur une liste établie et mise à jour à cet effet ;
- renforcer la sécurité de cette zone, en dehors des heures ouvrables, par la mise en œuvre de moyens de détection d'intrusion physique ;
- communiquer au Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information la localisation de cette zone, la description des dispositifs de sécurité mis en place et la liste du personnel autorisé à y accéder ;
- en cas de constatation de toute intrusion ou de toute tentative d'intrusion visant à pénétrer dans cette zone, ouvrir une enquête interne et, le cas échéant, déposer une plainte auprès de l'autorité compétente dans les vingt-quatre (24) heures qui suivent.

Article 24 :

Le prestataire prépare et tient à jour des manuels détaillés décrivant les procédures à suivre pour toutes ses activités et doit s'y conformer. Ces manuels doivent être communiqués, sur sa demande, au Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information.

Article 25 : Sécurité des prestations

Le prestataire s'engage à définir et à appliquer des procédures administratives et techniques visant à garantir la sécurité et la disponibilité des conventions secrètes et à prévenir tout manquement de la part de ses agents.

A cet effet, il élabore et tient à jour un document décrivant sa politique de sécurité, qui comporte, notamment :

- ses objectifs de sécurité, en particulier ceux concernant son activité principale et la gestion des conventions secrètes ;

- les règles de sécurité et le rappel des sanctions disciplinaires et pénales applicables en cas de manquement à ces règles ;

- la présentation de l'organisation de sécurité interne adoptée, en particulier les procédures :

    - d'information avec l'élaboration d'un guide pratique de sécurité à l'intention du personnel ;
    - de responsabilisation du personnel avec la désignation d'un responsable de la sécurité de l'organisme;
    - d'audits internes et de contrôles de l'application des règles de sécurité ;
    - du traitement des incidents signalés.

Article 26 : Sécurité informatique

Lorsque le prestataire emploie un système informatique, pour accomplir des fonctions de détention, de mise en œuvre et de remise des conventions secrètes de cryptographie, il s'engage à n'utiliser ledit système pour aucune autre application.

Il doit s'assurer que le système comporte des fonctions de sécurité permettant :

- l'identification et l'authentification des utilisateurs des systèmes informatiques ;
- la limitation des droits d'accès au strict besoin du service. Pendant toute la durée de leur détention, les conventions secrètes sont chiffrées. Elles ne sont déchiffrées que pour être mises en œuvre ou remises ;
- l'imputabilité de toute opération permettant d'accéder aux conventions secrètes ou autres ressources de sécurité du système à son auteur ;
- l'audit au moyen d'un enregistrement, sauvegardé régulièrement et archivé, de toute opération permettant l'accès aux conventions secrètes ou aux autres ressources de sécurité du système ;
- la mise à zéro au moyen d'un dispositif, de tous les objets de stockage ayant contenu une ressource sensible du système informatique avant toute utilisation ultérieure desdits objets. Lorsqu'il n'est plus utilisé, le dispositif de mise à zéro est détruit et sa destruction fait l'objet d'un compte rendu.

Le prestataire doit disposer d'un lieu sécurisé spécialement aménagé, pour la conservation des dispositifs servant à déchiffrer les conventions secrètes et dont l'accès est réservé aux seules personnes qu'il a autorisées.

Article 27 :

Le prestataire 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, aussi bien pour les systèmes de sauvegarde et

de traitement des informations fournies par les clients, que pour les systèmes de cryptographie.

Article 28 :

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.