REPUBLIQUE DU SENEGAL
Un peuple – Un but – Une foi

PRESIDENCE DE LA REPUBLIQUE

SECRETARIAT GENERAL

N° 2012-1508

Décret modifiant et complétant le décret n° 2010-1209 du 13 septembre 2010 relatif à la loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal

LE PRESIDENT DE LA REPUBLIQUE

Vu la Constitution ;

Vu la loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal ;

Vu la loi n° 2011-01 du 24 février 2011 portant Code des Télécommunications ;

Vu le décret n° 2007-909 du 31 juillet 2007 relatif à l'organisation de la Présidence de la République, modifié ;

Vu le décret n° 2010-1209 du 13 septembre 2010 relatif à la loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal ;

Vu le décret n° 2012-427 du 03 avril 2012 portant nomination du Premier Ministre ;

Vu le décret n° 2012-428 du 03 avril 2012 portant nomination du Ministre d'Etat, Secrétaire Général de la Présidence de la République ;

Vu le décret n° 2012-1163 du 29 octobre 2012 relatif à la composition du Gouvernement ;

Vu le décret n° 2012-1223 du 5 novembre 2012 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,

DECRETE

Article premier : L'article 9 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« En application de l'article 8 de la loi n° 2008-41 du 20 août 2008 sur la cryptologie au Sénégal, les membres de la Commission nationale de Cryptologie reçoivent une indemnité de session fixée par arrêté du Président de la République sur proposition conjointe du Président de ladite commission et du Directeur général de l'Autorité de Régulation des Télécommunications et des Postes. »

Article 2 : L'article 13 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« Toutes les opérations utilisant des moyens ou des prestations de cryptologie dispensées de toute formalité préalable par la Commission nationale de Cryptologie sont libres.

Les catégories des moyens et des prestations de cryptologie concernées, ainsi que lesdites opérations, sont indiquées respectivement dans la première et la deuxième colonne du tableau à l'annexe I du présent décret.

L'utilisation privée, par une personne physique, de logiciel de cryptographie avec des clefs de longueur inférieure ou égale à 128 bits est également libre**. »**

Article 3 : L'article 19 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« La forme et le contenu du dossier de déclaration figurent à l'annexe II du présent décret.

Tout autre document jugé nécessaire peut être demandé par la Commission nationale de Cryptologie à tout moment de la procédure de déclaration. »

Article 4 : L'article 21 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« En application de l'article 15 de la loi n° 2008-41du 20 août 2008 sur la Cryptologie au Sénégal, le régime d'autorisation porte sur l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité.

Le régime d'autorisation porte également sur toute opération de fourniture, d'importation ou d'utilisation de moyen ou de prestation de cryptologie avec une longueur de clef supérieure à 128 bits. »

Article 5 : L'article 32 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« La forme et le contenu du dossier de demande d'autorisation figurent à l'annexe II du présent décret.

Tout autre document jugé nécessaire peut être demandé par la Commission nationale de Cryptologie à tout moment de la procédure d'autorisation. »

Article 6 : L'article 47 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« Les dossiers de demande d'agrément présentés par les organismes qui envisagent de gérer, pour le compte d'autrui, des conventions secrètes, doivent comporter :

1) l'ensemble des pièces attestant de l'identité et de la structure juridique de l'organisme demandeur d'agrément de prestations de cryptologie :
    - nom, dénomination ;
    - raison sociale ;
    - adresse du siège social, numéro de téléphone, adresse email, numéro d'identification nationale des entreprises et associations (NINEA) ;
    - extrait du registre du commerce, fiche individuelle d'état civil et de nationalité de chaque associé, éventuellement ;
    - répartition des parts sociales de la société ;
    - copie des textes portant création de l'organisme ;
2) un document décrivant la politique de sécurité mise en place par l'organisme, conformément aux articles 57 et 58 du décret n° 2010-1209 du 13 septembre 2010 ;
3) un exemplaire signé du cahier des charges dans les conditions prévues à l'article 7 du présent décret.
4) le contrat type que l'organisme propose à ses clients conformément à l'article 8 du présent décret ;

Si le dossier est complet, le Président de la Commission nationale de Cryptologie notifie la décision prise dans un délai de quatre mois à compter de la date de réception du dossier.

A défaut de notification dans ce délai, le silence de la Commission nationale de Cryptologie vaut rejet du dossier de demande d'agrément.

Le dossier de demande d'agrément est réputé complet si, dans le délai d'un mois suivant la réception, la Commission nationale de Cryptologie n'a pas invité le demandeur à fournir des pièces complémentaires nécessaires.

Dans ce dernier cas, le délai de quatre mois part dès la réception des pièces complétant le dossier. »

Article 7 : L'article 51 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« Tout agrément suppose le respect d'un cahier des charges comprenant notamment :

1) l'énumération des moyens ou des prestations de cryptologie dont l'organisme agréé est autorisé à gérer les conventions secrètes ;
2) l'énumération des moyens ou des prestations de cryptologie que l'organisme agréé peut utiliser ou fournir ;
3) les conditions techniques ou administratives garantissant le respect des obligations imposées à l'organisme agréé ;
4) le nombre de personnes mentionnées à l'article 48 du décret n° 2010-1209 du 13 septembre 2010 ;
5) les conditions de transfert à un autre organisme agréé des conventions secrètes en cas de cessation d'activité, de retrait d'agrément ou à la demande de l'utilisateur ;
6) le format électronique standardisé dans lequel doivent être transcrites les conventions secrètes en cas de cessation d'activité ou de retrait d'agrément ;
7) les dispositions techniques prises lors de la mise en service des conventions secrètes afin d'identifier l'organisme agréé gérant lesdites conventions ainsi que les utilisateurs concernés ;
8) les conditions techniques d'utilisation des conventions secrètes, des moyens ou des prestations et les mesures nécessaires pour assurer leur intégrité et leur sécurité.

Le cahier des charges comporte également une annexe sur les modalités pratiques, ci-après, de remise des conventions secrètes aux autorités administratives et judiciaires compétentes ou de leur mise en œuvre à la demande desdites autorités :

1) le personnel responsable de la mise en œuvre ou de la remise des conventions secrètes ;
2) le lieu de remise des conventions secrètes ;
3) le lieu de mise en œuvre des conventions secrètes ;
4) les moyens de cryptologie utilisés pour la mise en œuvre des conventions secrètes ;
5) la tenue et la présentation du registre des demandes de remise ou de mise en œuvre des conventions secrètes conformément aux articles 55 et 56 du décret n° 2010-1209 du 13 septembre 2010 ;
6) les conditions techniques de la mise en œuvre.

A l'exception de son annexe, le contenu de ce cahier des charges peut être communiqué, sur leur demande, aux utilisateurs dont l'organisme agréé gère les conventions secrètes. »

Article 8 : L'article 54 du décret n° 2010-1209 du 13 septembre 2010 est abrogé et remplacé par les dispositions suivantes :

« La signature d'un contrat de gestion des conventions secrètes est obligatoire entre l'organisme agréé et l'utilisateur.

Ce contrat comprend obligatoirement :

1) la référence de l'agrément, la durée et la date d'expiration ainsi que tout élément d'information jugée utile par le cahier des charges ;
2) la mission de l'organisme agréé, notamment la gestion, pour le compte des clients, de conventions secrètes permettant d'assurer la confidentialité (détention, conservation certification, et éventuellement génération des clefs) et restitution des données au client ou à la demande des autorités administratives et judiciaires;
3) un engagement de l'organisme agréé relatif à la confidentialité ou à la sécurité des conventions secrètes qu'il gère pour le compte de l'utilisateur ;
4) le lieu de gestion des conventions secrètes ;
5) les informations légales et réglementaires à communiquer aux clients notamment les sanctions encourues par ceux-ci en cas de mauvais usage ou de détournement du moyen dont le prestataire gère les conventions secrètes ;
6) le droit d'accès du client aux informations le concernant ;
7) l'engagement de l'organisme agréé à communiquer au client, en cas de cessation d'activité ou de retrait d'agrément, la liste des organismes agréés offrant les mêmes services ;
8) les règles d'emploi détaillées des moyens de cryptologie proposés aux clients sous forme de manuel indiquant la procédure de chiffrement et de génération des clefs employées ;
9) les modalités selon lesquelles l'utilisateur, ou toute autre personne éventuellement mandatée par celui-ci, pourra, à sa demande, se faire délivrer une copie de ses conventions secrètes. »

Article 9 :

Le Premier Ministre et le Ministre d'Etat, Secrétaire général de la Présidence de la République sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret qui sera publié au journal officiel.

Fait à Dakar, le **31 décembre 2012**

Par le Président de la République **Macky SALL**

Le Premier Ministre

Abdoul MBAYE

R E P U B L I Q U E D U S E N E G A L
UN PEUPLE - UN BUT - UNE FOI

PRESIDENCE DE LA REPUBLIQUE

S E C R E T A R I A T G E N E R A L

ANNEXE I

Les catégories de moyens et de prestations de cryptologie dont les opérations sont dispensées de toute formalité préalable

NR	MOYENS OU PRESTATIONS	OPERATIONS DISPENSEES DE TOUTE FORMALITE PREALABLE
1.	Moyens ou prestations conçus pour protéger des mots de passe, des codes d'identification personnels ou des données d'authentification similaires, utilisés uniquement pour contrôler l'accès à des données, à des ressources, à des services ou à des locaux, sous réserve qu'ils ne permettent de chiffrer que les fichiers de mots de passe ou de codes d'identification et les informations nécessaires au contrôle d'accès.	- Fourniture - Utilisation - Exportation - Importation
2.	Moyens ou prestations conçus pour élaborer ou protéger une procédure de signature, une valeur de contrôle cryptographique, un code d'authentification de message ou une information similaire, pour vérifier la source des données, prouver la remise des données au destinataire, ou bien détecter les altérations ou modifications subreptices portant atteinte à l'intégrité des données, sous réserve qu'ils ne permettent de chiffrer que les informations nécessaires à l'authentification ou au contrôle d'intégrité des données concernées.	- Fourniture - Utilisation - Exportation - Importation
3.	Matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur inférieure ou égale à 128 bits, à condition que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, leur fournisseur ou leur importateur et que les conventions secrètes soient gérées par un organisme agréé par la Commission nationale de Cryptologie.	Utilisation privée par une personne physique

4.	Equipements conçus ou modifiés pour utiliser la cryptologie faisant appel à des techniques analogiques tels que : a. Equipements utilisant des techniques de mélange de bandes " fixes" ne dépassant pas 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; b. Equipements utilisant des techniques de mélange de bandes " fixes " dépassant 8 bandes et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les dix secondes ; c. Equipements utilisant l'inversion à fréquence « fixe » et où les changements de transposition ne s'effectuent pas plus d'une fois toutes les secondes ; d. Equipements de radiodiffusion pour audience restreinte ; e. Equipements de télévision civile.	- Utilisation - Importation
5.	Cartes à microprocesseur personnalisées ou leurs composants spécialement conçus, incapables de chiffrer le trafic de messages ou les données fournies par l'utilisateur ou leur prestation de gestion de clef associée.	- Fourniture - Utilisation - Exportation - Importation
6.	Equipements de réception de télévision de type grand public, sans capacité de chiffrement numérique et où le déchiffrement numérique est limité aux fonctions vidéo, audio ou de gestion.	- Fourniture - Utilisation - Exportation - Importation
7.	Equipements autonomes de lecture de disques vidéo numériques, de type grand public, sans capacité de chiffrement, où le déchiffrement est limité aux informations vidéo, audio, informatiques et de gestion	- Fourniture - Utilisation - Exportation - Importation
8.	Moyens matériels ou logiciels spécialement conçus pour assurer la protection des logiciels contre la copie ou l'utilisation illicite, dont les fonctions de déchiffrement ne sont pas accessibles à l'utilisateur.	- Fourniture - Utilisation - Exportation - Importation

9.	Equipements de contrôle d'accès, tels que machines automatiques de distribution de billets, imprimantes libre-service de relevés de compte ou terminaux de points de vente, protégeant les mots de passe, numéros d'identification personnels ou autres données similaires empêchant l'accès non autorisé à des installations, mais ne permettant pas le chiffrement des fichiers ou des textes, sauf lorsqu'il est directement lié à la protection des mots de passe ou des numéros d'identification personnels.	- Fourniture - Utilisation - Exportation - Importation
10.	Systèmes de gestion de facturation inclus dans les dispositifs de relevés de compteurs dont les fonctions de chiffrement sont directement liées au comptage.	- Fourniture - Utilisation - Exportation - Importation
11.	Equipements dotés de moyens de cryptologie lorsqu'ils accompagnent les personnalités étrangères sur invitation officielle de l'Etat du Sénégal.	- Utilisation - Exportation - Importation
12.	Stations de base de radiocommunications cellulaires commerciales civiles limitées au raccordement de radiotéléphones, et qui ne permettent pas d'appliquer des techniques cryptographiques au trafic de messages entre terminaux mobiles, sauf sur les liens directs entre radiotéléphones et stations de bases (connues sous le nom d'interface radio)	- Fourniture - Utilisation - Exportation - Importation
13.	Radiotéléphones portatifs ou mobiles destinés à l'usage civil qui ne sont pas en mesure de procéder au chiffrement de bout en bout.	- Fourniture - Utilisation - Exportation - Importation
14.	Equipements, destinés au grand public, permettant d'échanger entre eux des données par radiocommunications, et lorsque les seules capacités cryptographiques de l'équipement sont conçues conformément aux normes nationales et internationales validées par la Commission nationale de Cryptologie.	- Fourniture - Utilisation - Exportation - Importation

REPUBLIQUE DU SENEGAL
UN PEUPLE - UN BUT - UNE FOI

PRESIDENCE DE LA REPUBLIQUE

SECRETARIAT GENERAL

ANNEXE II

Forme et contenu du dossier de déclaration ou de demande d'autorisation de fourniture, d'exportation, d'importation ou d'utilisation d'un moyen ou d'une prestation de cryptologie

Le formulaire doit être adressé en trois exemplaires au Secrétariat Général de la Présidence de la République, Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information (Commission nationale de Cryptologie) 1, Avenue Léopold Sédar Senghor,
BP 4026 Dakar
Téléphone : 33 880 83 47/ 33 821 49 75 / 33 880 83 45
Télécopie : 33 823 28 40/ 33 821 86 60,
Mail: stccam@stcc-ssi.sn
Site: www.stcc-ssi.sn

Numéro de dossier (réservé à l'administration) : ……

A°) DECLARATION D'OPERATION RELATIVE A UN MOYEN DE CRYPTOLOGIE

Déclaration :

- ❑ de fourniture d'un moyen de cryptologie :
- ❑ d'importation en provenance de……
  - ❑ en vue de la fourniture d'un moyen de cryptologie pour une durée de …… .. (cinq ans au maximum) ;
  - ❑ en vue d'une prestation de cryptologie pour une durée de …… …… (cinq ans maximum) ;
  - ❑ en vue d'utilisation pour une durée de …… ……. (trois mois au maximum) ;
  - ❑ en vue d'une exportation pour une durée de … …… (trois mois au maximum) à destination de ……
- ❑ de renouvellement en cas de :
  - ❑ modification des caractéristiques techniques ;
  - ❑ changement de nom commercial ;
  - ❑ changement technique du moyen de cryptologie ;
  - ❑ fin de la période de validité de la déclaration.

A.1°/ Déclarant

A.1.1 Société

Joindre un document présentant la société, un extrait du registre de commerce datant de moins de trois mois (ou un document équivalent pour les sociétés de droit étranger), une facture SDE, SENELEC ou SONATEL au nom du déclarant avec indication du domicile et une copie légalisée de la Carte nationale d'Identité :

Nom : ……
Raison sociale : ……..
Nationalité : …….
NINEA : ……
Adresse : ……
Numéro de téléphone : ……..
Numéro de télécopie : ……
Adresse du courrier électronique : …….
Adresse du site internet :……

Personne chargée du dossier administratif

Prénoms et nom *:* ……
Nationalité : …….
Adresse *:* …….
Numéro de téléphone : ……
Adresse du courrier électronique : ……..

A.1.2 Particulier

Joindre : Une facture SDE, SENELEC ou SONATEL au nom du déclarant avec indication du domicile et une copie légalisée de la Carte nationale d'Identité.

Prénoms et nom : …….
Nationalité : ……
Adresse *:* ……..
Numéro de téléphone : ……
Adresse du courrier électronique : ……..

A.2°/ <u>Moyen de cryptologie objet de la déclaration</u>

A.2.1 Moyen de cryptologie

Joindre une brochure commerciale du moyen de cryptologie et le manuel utilisateur

Référence commerciale : ……..
Référence constructeur **:** ……..
Version **:** ……
Description succincte du moyen et de ses fonctionnalités **:** ……
……
Catégorie du moyen de cryptologie :

- ❑ Logiciel de chiffrement pour ordinateur personnel
- ❑ Système d'exploitation
- ❑ Messagerie électronique
- ❑ Système de chiffrement au niveau du réseau
- ❑ Téléphone ou télécopie
- ❑ Autres (à préciser) : ……..

A.2.2 Fabricant du moyen de cryptologie (si différent du déclarant)

Nom **:** ……
Nationalité : …….
Raison sociale **:** ……...
Adresse **:** …….
Numéro de téléphone : ……
Numéro de télécopie **:** ……
Adresse du courrier électronique **:** …….

A.2.3 Personne chargée du dossier technique

Joindre : Une facture SDE, SENELEC ou SONATEL au nom de la personne chargée du dossier technique avec indication du domicile et une copie légalisée de la Carte nationale d'Identité :

Prénoms et nom **:** …….
Adresse : ……
Numéro de téléphone **:** ……
Numéro de télécopie **:** …….
Adresse du courrier électronique **:** ……..

A.2.4 Services de cryptologie fournis

- ❑ Intégrité ……
- ❑ Authentification ……
- ❑ Signature ……
- ❑ Confidentialité ……..
- ❑ Contrôle d'accès ……
- ❑ Autre(s) à préciser : ……..

A.2.5 Mise en œuvre des algorithmes

- ❑ Logiciel.
- ❑ Matériel (à préciser) *:* …….

A.2.6 Normes ou standards de sécurité du moyen

- ❑ Normes ou standards (à préciser) : ……

A.3°/ <u>ATTESTATION</u>

Je soussigné (prénoms, nom) ……..…….. agissant en qualité de ……. , pour le compte de ……..……., représentant le déclarant, certifie que les renseignements figurant sur cette déclaration et qui y sont joints, sont exacts et ont été établis de bonne foi, et que le déclarant s'engage à porter à la connaissance de la Commission nationale de Cryptologie, sans délai, tout élément nouveau de fait ou de droit de nature à modifier cette déclaration ou les éléments joints, toute modification, toute fausse déclaration ou tout manquement aux engagements souscrits m'exposant aux sanctions prévues aux articles 19 et 20 de la Loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal.

Date : ……..

<u>Signature</u>

<u>Eléments techniques à joindre au dossier de déclaration d'opération relative à un moyen de cryptologie</u>

1. **Les éléments nécessaires pour mettre en œuvre le moyen de cryptologie** :
    a. Deux exemplaires du matériel de cryptologie ou du logiciel concerné ;
    b. Les guides d'installation du moyen de cryptologie ;
    c. Les dispositifs d'activation du moyen, s'il y a lieu (numéro de licence, numéro d'activation, dispositif matériel, etc. …) ;
    d. Les dispositifs d'injection de clé ou d'activation du réseau, s'il y a lieu.
2. **Les éléments relatifs aux algorithmes cryptographiques** :
    a. La description des fonctions de cryptologie offertes par le moyen (chiffrement, signature, gestion de clés, ...) ;
    b. Soit la description complète des procédés de cryptologie employés, sous la forme d'une description synoptique et mathématique et d'une simulation dans un langage de haut niveau ; soit la référence à un dossier préalablement déposé pour un moyen employant les mêmes procédés de cryptologie ; soit la référence à un standard reconnu, non équivoque, et dont les détails techniques sont accessibles aisément et sans condition , avec les paramètres et les modes opératoires de sa mise en œuvre ;
    c. Si le procédé de chiffrement mis en œuvre dans le moyen n'est pas un standard reconnu, trois sorties de référence du procédé de chiffrement, sous format électronique, à partir d'un texte clair et d'une clé choisie arbitrairement, qui seront fournis, dans le but de vérifier la conformité de la mise en œuvre du procédé à la description de celui-ci.
3. **Les éléments relatifs à la gestion des clefs**
    a. Le procédé de génération et de mise à jour des clés ;
    b. Le mode de distribution des clés ;
    c. Le format de transmission des clés ;
    d. Le format de conservation des clés ;
    e. Le mode de destruction des clés ;
    f. La longévité des clés.
4. **Les éléments relatifs à la protection du procédé de chiffrement** à savoir la description des mesures techniques mises en œuvre pour empêcher l'altération du procédé de chiffrement ou de la gestion de clés associée.
5. **Les éléments relatifs au traitement des données** :
    a. La description des prétraitements subis par les données claires avant leur chiffrement (compression, formatage, ajout d'un en-tête, etc.) ;
    b. La description des post-traitements des données chiffrées, après leur chiffrement (ajout d'un en-tête, formatage, mise en paquet, etc.) ;
    c. Trois sorties de référence du moyen, sous format électronique, effectuées à partir d'un texte clair et d'une clé choisie arbitrairement, qui seront aussi fournis dans le but de vérifier la mise en œuvre du moyen par rapport à la description de celui-ci.
6. **Les éléments relatifs à la mise en œuvre de la cryptologie** (à ne fournir que sur demande de la Commission nationale de Cryptologie)**:**
    a. Le code source du moyen, et les éléments permettant une recompilation du code source ou les références des compilateurs associés ;
    b. Les références des composants intégrant les fonctions de cryptologie du moyen et les noms des fabricants de chacun de ces composants ;
    c. Les fonctions de cryptologie mises en œuvre par chacun de ces composants ;
    d. La documentation technique du ou des composants réalisant les fonctions de cryptologie ;
    e. Les types des mémoires (flash, ROM, EPROM, etc.) dans lesquelles sont stockées les fonctions et les paramètres de cryptologie ainsi que les références de ces mémoires.

B°) DECLARATION DE FOURNITURE D'UNE PRESTATION DE CRYPTOLOGIE

B.1°/ Déclarant

B.1.1/ Société

Joindre un document présentant la société, un extrait du registre de commerce datant de moins de trois mois (ou un document équivalent pour les sociétés de droit étranger), une facture SDE, SENELEC ou SONATEL au nom du déclarant avec indication du domicile et une copie légalisée de la Carte nationale d'Identité.

Nom : ……
Raison sociale : ……..
Nationalité : …….
NINEA : ……
Adresse : ……
Numéro de téléphone : ……..
Numéro de télécopie : ……
Adresse du courrier électronique : …….
Adresse du site internet :……

Personne chargée du dossier administratif

Prénoms et nom *:* ……
Nationalité : …….
Adresse *:* …….
Numéro de téléphone : ……
Adresse du courrier électronique : ……..

B.1.2 Particulier

Joindre : Une facture SDE, SENELEC ou SONATEL au nom du déclarant avec indication du domicile et une copie légalisée de la Carte Nationale d'Identité.

Prénoms et nom : …….
Nationalité : ……
Adresse *:* ……
Numéro de téléphone : ……
Adresse du courrier électronique : ……..

B.2°/ Description de la prestation :

B.2.1 Catégories d'utilisateurs auxquelles est destinée la prestation :

- ❑ Administrations (préciser) ……..
- ❑ Grandes entreprises (préciser) …….
- ❑ Etablissements financiers (préciser) …….
- ❑ PME (préciser) …….
- ❑ Professions libérales (préciser) ……
- ❑ Autres (préciser avec le secteur d'activité) ……

B.2.2 Types de données concernées par la prestation :

Préciser le type de données concernées par la prestation (données personnelles, médicales, financières, administratives, … autres) : ……
…….

B.2.3 Services de cryptologie fournis

Préciser les noms des algorithmes utilisés et la longueur maximale des clés cryptographiques pour chaque algorithme :

- ❑ Intégrité
- ❑ Authentification ……
- ❑ Signature ……
- ❑ Confidentialité …….
- ❑ Archivage sécurisé ……..
- ❑ Gestion des clés cryptographiques
- ❑ Certification de clés ou de données
- ❑ Autre(s) à préciser : ……..

B.2.4 Personne chargée du dossier technique

Joindre : Une facture SDE, SENELEC ou SONATEL au nom de la personne chargée du dossier technique avec indication du domicile et une copie légalisée de la Carte nationale d'Identité.

Prénoms et nom : ……
Nationalité : ……..
Adresse : ……
Numéro de téléphone : ……
Numéro de télécopie : ……
Adresse du courrier électronique : ……

B.3°/ <u>Moyens cryptologiques mis en œuvre par le prestataire pour fournir sa prestation</u> :

- ❑ Référence commerciale des moyens :
- ❑ Référence constructeur des moyens :
- ❑ Version : …….

  Le cas échéant, référence des déclarations ou des autorisations relatives aux moyens : .....
  ……

B.4 °/ <u>ATTESTATION</u>

Je soussigné (prénoms, nom) …… ……. …….. agissant en qualité de ……., pour le compte de …….. ……., représentant le déclarant, certifie que les renseignements figurant sur cette déclaration qui y sont joints, sont exacts et ont été établis de bonne foi, et que le déclarant s'engage à porter à la connaissance de la Commission nationale de Cryptologie, sans délai, tout élément nouveau de fait ou de droit de nature à modifier cette déclaration ou les éléments joints, toute modification, toute fausse déclaration ou tout manquement aux engagements souscrits m'exposant aux sanctions prévues aux articles 19 et 20 de la Loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal.

Date : ……..

<u>Signature</u>

<u>Eléments techniques à joindre à la déclaration de fourniture d'une prestation de cryptologie</u>

1. La description des services offerts aux utilisateurs de la prestation ;
2. La description des fonctions cryptologiques mises en œuvre par le prestataire ;
3. La description des locaux utilisés pour mettre en œuvre la prestation ;
4. La description des matériels et logiciels informatiques et notamment des moyens de cryptologie utilisés par le prestataire ;
5. La description des systèmes de protection physique et de contrôle d'accès aux locaux et aux systèmes informatiques du prestataire ;
6. Lorsque la prestation consiste en la gestion des clefs cryptographiques ou des certificats électroniques au profit des utilisateurs :
   a. La description de la procédure de génération des clefs et des certificats ;
   b. La description de la procédure de distribution et de remise des clefs et des certificats aux utilisateurs ;
   c. La description des mesures techniques et organisationnelles mises en œuvre pour la protection et la conservation des clefs ;
   d. La description de la procédure de recouvrement des clés (uniquement pour la confidentialité) ;
   e. Les références des moyens de cryptologie mis en œuvre par les utilisateurs de la prestation, lorsque ces moyens sont spécifiquement conçus pour fonctionner avec les clefs ou les certificats délivrés par ce prestataire agréé par la Commission nationale de Cryptologie (Article 12 de la loi n° 2008-41 du 20 août 2008).

C°/ DEMANDE D'AUTORISATION D'OPERATION RELATIVE A UN MOYEN DE CRYPTOLOGIE

Demande d'autorisation :

- ❑ de fourniture pour une durée de ..... (cinq ans au maximum) en vue de l'utilisation :
  - ❑ individuelle
  - ❑ collective
- ❑ d'importation pour une durée de ..... (cinq ans au maximum) en provenance de …….
- ❑ d'exportation pour une durée de ..... (cinq ans au maximum) à destination de ……
- ❑ d'utilisation à usage :
  - ❑ individuelle pour une durée de ..... (cinq ans au maximum)
  - ❑ collective pour une durée de ..... (dix ans au maximum)

- ❑ de renouvellement en cas de :
  - ❑ modification des caractéristiques techniques ;
  - ❑ changement de nom commercial ;
  - ❑ changement technique du moyen de cryptologie ;
  - ❑ fin de la période de validité de l'autorisation.

C.1°/ Demandeur d'autorisation

C.1.1 Société

Joindre un document présentant la société, un extrait du registre de commerce datant de moins de trois mois (ou un document équivalent pour les sociétés de droit étranger), une facture SDE, SENELEC ou SONATEL au nom du déclarant avec indication du domicile et une copie légalisée de la Carte nationale d'Identité.

Dénomination sociale : .....
NINEA : .....
Nationalité : .....
Adresse : .....
Numéro de téléphone : .....
Numéro de télécopie : .....
Adresse du courrier électronique : .....
Adresse du site internet : .....

Personne chargée du dossier administratif

Nom et prénoms : .....
Nationalité : .....
Adresse : .....
Numéro de téléphone : .....
Numéro de télécopie : .....
Adresse du courrier électronique : .....

C.1.2. Particulier

Joindre : Une facture SDE, SENELEC ou SONATEL au nom du déclarant avec indication du domicile et une copie légalisée de la Carte nationale d'Identité.

Prénoms et Nom : .....
Nationalité : .....
Adresse : .....
Numéro de téléphone : .....
Numéro de télécopie : .....
Adresse du courrier électronique : .....

C.2°/ Moyen de cryptologie auquel s'applique la demande d'autorisation

C.2.1. Moyen de cryptologie

Joindre une brochure commerciale du moyen de cryptologie et le manuel utilisateur :
Référence commerciale : .....
Référence constructeur : .....
Version : .....
Description générale du moyen et de ses fonctionnalités : .....
.....
Classer le moyen de cryptologie dans une ou plusieurs des catégories proposées ci-dessous :

- ❑ Logiciel de chiffrement pour ordinateur personnel.
- ❑ Système d'exploitation.
- ❑ Messagerie électronique.
- ❑ Système de communication sans fil.
- ❑ Moyen de chiffrement au niveau du réseau.
- ❑ Téléphone ou télécopie.
- ❑ Autres (à préciser).....

C.2.2. Fabricant du moyen de cryptologie (si différent du demandeur d'autorisation)

Dénomination sociale : .....
NINEA : .....
Nationalité : .....
Adresse : .....
Numéro de téléphone : .....
Numéro de télécopie : .....
Adresse du courrier électronique : .....
Adresse du site internet : .....

C.2.3. Personne chargée des éléments techniques

Joindre : Une facture SDE, SENELEC ou SONATEL au nom de la personne chargée du dossier technique avec indication du domicile et une copie légalisée de la Carte Nationale d'Identité.
Nom et prénoms : .....
Nationalité : .....
Adresse : .....
Numéro de téléphone : .....
Numéro de télécopie : .....
Adresse du courrier électronique : .....

C.2.4. Services de cryptologie fournis

Préciser les noms des algorithmes utilisés et la longueur maximale des clés cryptographiques pour chaque algorithme :

- ❑ Intégrité :.....
- ❑ Authentification :.....
- ❑ Signature : .....
- ❑ Confidentialité : .....
- ❑ Autres (à préciser) : .....

C.2.5. Mise en œuvre des algorithmes

- ❑ Logiciel.
- ❑ Matériel (à préciser) : .....

C.2.6. Normes ou standards de sécurité du moyen

- ❑ Normes ou standards (à préciser) : .....

C.3 **Attestation**

Je soussigné (prénoms, nom) : ..... agissant en qualité de : ..... pour le compte de ..... , représentant le demandeur d'autorisation, certifie que les renseignements figurant sur cette demande d'autorisation et qui y sont joints, sont exacts et ont été établis de bonne foi, et que le demandeur s'engage à porter à la connaissance à la Commission nationale de Cryptologie, sans délai, tout élément nouveau de fait ou de droit de nature à modifier cette demande ou les éléments joints, toute omission ou toute fausse déclaration exposant le demandeur aux sanctions prévues aux articles 19 et 20 de la loi n° 2008-41 du 20 août 2008.

Date : .....

Signature

Eléments techniques à joindre à la demande d'autorisation d'une opération relative à un moyen de cryptologie

1. Les éléments nécessaires pour mettre en œuvre le moyen de cryptologie :
    a. La référence commerciale du produit :
    b. Deux exemplaires du matériel de cryptologie ou du logiciel concerné ;
    c. Les guides d'installation du moyen ;
    d. Les dispositifs d'activation du moyen, s'il y a lieu (numéro de licence, numéro d'activation, dispositif matériel, etc.) ;
    e. Les dispositifs d'injection de clé ou d'activation du réseau, s'il y a lieu.
2. Les éléments relatifs aux algorithmes cryptographiques :
    a. La description des fonctions de cryptologie offertes par le moyen (chiffrement, signature, gestion de clés, etc.) ;
    b. Soit la description complète des procédés de cryptologie employés, sous la forme d'une description synoptique et mathématique et d'une simulation dans un langage de haut niveau ; Soit la référence à un dossier préalablement déposé pour un moyen employant les mêmes procédés de cryptologie ; Soit la référence à un standard reconnu, non équivoque, et dont les détails techniques sont accessibles aisément et sans condition, avec les paramètres et les modes opératoires de sa mise en œuvre ;
    c. Si le procédé de chiffrement mis en œuvre dans le moyen n'est pas un standard reconnu, trois sorties de référence du procédé de chiffrement, sous format électronique, à partir d'un texte clair et d'une clé choisie arbitrairement, qui seront aussi fournis, dans le but de vérifier la conformité de la mise en œuvre du procédé à la description de celui-ci.
3. Les éléments relatifs à la gestion des clés :
    a. Le procédé de génération et de mise à jour des clés ;
    b. Le mode de distribution des clés ;
    c. Le format de transmission des clés.
    d. Le format de conservation des clés ;
    e. Le mode de destruction des clés ;
    f. La longévité des clés.
4. Les éléments relatifs à la protection du procédé de chiffrement, à savoir la description des mesures techniques mises en œuvre pour empêcher l'altération du procédé de chiffrement ou de la gestion de clés associée.
5. Les éléments relatifs au traitement des données :
    a. La description des prétraitements subis par les données claires avant leur chiffrement (compression, formatage, ajout d'un en-tête, etc.) ;
    b. La description des post-traitements des données chiffrées, après leur chiffrement (ajout d'un en-tête, formatage, mise en paquet, etc.) ;
    c. Trois sorties de référence du moyen, sous format électronique, effectuées à partir d'un texte clair et d'une clé choisie arbitrairement, qui seront aussi fournis, dans le but de vérifier la mise en œuvre du moyen par rapport à la description de celui-ci.
6. Les éléments relatifs à la mise en œuvre de la cryptologie (à ne fournir que sur demande de la Commission nationale de Cryptologie) :
    a. Le code source du moyen, et les éléments permettant une recompilation du code source ou les références des compilateurs associés ;
    b. Les références des composants intégrant les fonctions de cryptologie du moyen et les noms des fabricants de chacun de ces composants ;
    c. Les fonctions de cryptologie mises en œuvre par chacun de ces composants ;

d. La documentation technique du ou des composants réalisant les fonctions de cryptologie ; Les types des mémoires (flash, ROM, EPROM, etc.) dans lesquelles sont stockés les fonctions et les paramètres de crypto.