

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) :

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
- d'exportation pour une durée de (cinq ans au maximum) à destination
- 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

Éléments 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.