

ACTOBA

Base juridique des Médias et des réseaux de Communication

w w w . a c t o b a . c o m

Arrêté du 17 mars 1999

Définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie

Le Premier ministre,

Vu la loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;

Vu le décret no 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, notamment ses articles 5, 10 et 13,

Arrête :

Article 1er

Le dossier de déclaration ou de demande d'autorisation concernant un moyen ou une prestation de cryptologie comporte une partie administrative et une partie technique.

La partie administrative comprend une déclaration ou une demande d'autorisation conforme au modèle annexé au présent arrêté, en trois exemplaires.

La partie technique comprend une description conforme au modèle annexé au présent arrêté, en trois exemplaires. Sont joints à cette partie deux exemplaires du matériel concerné ou, pour les logiciels, un exemplaire de celui-ci.

Les dossiers déposés dans le cadre du régime simplifié de déclaration prévu à l'article 9 du décret du 24 février 1998 susvisé ainsi que ceux déposés pour obtenir le renouvellement d'une autorisation ne comportent pas de partie technique. Celle-ci est remplacée par un engagement écrit de la personne déposant le dossier certifiant soit que l'impossibilité pour le moyen ou la prestation d'assurer des fonctions de confidentialité ne résulte pas d'un simple dispositif de verrouillage, soit que les caractéristiques techniques du moyen ou de la prestation sont inchangées par rapport à la description figurant dans la partie technique du dossier déposé lors de la première délivrance de l'autorisation.

Article 2

Est porté à la connaissance du service central de la sécurité des systèmes d'information, au moins un mois à l'avance, tout changement de nature à modifier le contenu du dossier de déclaration ou de demande d'autorisation.

Article 3

L'arrêté du 13 mars 1998 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie est abrogé.

Article 4

Le secrétaire général de la défense nationale est chargé de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 17 mars 1999.

ANNEXE

PREMIER MINISTRE SERVICE CENTRAL DE
LA SECURITE DES SYSTEMES
D'INFORMATION

18, rue du Docteur-Zamenhof, 92131 Issy-les-Moulineaux Cedex (téléphone : 01-41-46-37-00, Fax : 01-41-46-37-01)

Numéro de dossier (*) :

Déclaration/Demande d'autorisation concernant un moyen ou une prestation de cryptologie

PARTIE ADMINISTRATIVE

Cocher la ou les cases correspondantes :

Déclaration simplifiée de fourniture en vue de l'utilisation générale en vue de l'exportation d'importation en provenance de :
.....d'utilisation personnelle

ACTOBA

La lettre juridique des Médias et des réseaux de Communication

w w w . a c t o b a . c o m

Demande d'autorisation de fourniture pour une durée de : (cinq ans maximum) d'un moyen ou d'une prestation qui n'utilise que des conventions secrètes gérées par un organisme agréé de fourniture pour une durée de : (cinq ans maximum) en vue de l'utilisation générale en vue de l'utilisation collective d'exportation pour une durée de : (cinq ans maximum) d'importation en provenance de : d'utilisation personnelle pour une durée de : (dix ans maximum)

(*) Réserve à l'administration.

A. - Déclarant ou demandeur d'autorisation

A.1. Société

Nom :

Raison sociale :

Nationalité :

Numéro SIRET :

Adresse :

Numéro de téléphone :

Numéro de télécopie :

Adresse du courrier électronique :

Personne chargée du dossier administratif :

Nom.....

Prénoms.....

Adresse :

Numéro de téléphone :

Numéro de télécopie :

Adresse du courrier électronique :

A.2. Particulier

Nom.....

Prénoms :

Nationalité :

Adresse :

Numéro de téléphone :

Adresse du courrier électronique :

B. - A renseigner selon les cas suivants

B.1. Demande d'autorisation de fourniture d'un moyen ou d'une prestation qui utilise des conventions secrètes gérées par un organisme agréé Référence de(s) organisme(s) agréé(s) :

B.2. Demande d'autorisation de fourniture en vue de l'utilisation collective Catégories éventuelles d'utilisateurs auxquels le moyen ou

la prestation est destiné :

Administrations (à préciser) :

Grandes entreprises (préciser secteur d'activités) :

Etablissements de crédit :

PME (préciser secteur d'activités) :

Autres (à préciser avec secteur d'activités) :

B.3. Demande d'autorisation d'utilisation personnelle Besoins justifiant la demande :

Lieux d'utilisation du moyen de cryptologie :

Le cas échéant, réseaux de télécommunications employés :

C. - Moyen ou prestation auquel s'applique la déclaration ou la demande d'autorisation

C.1. Moyen ou prestation de cryptologie

Référence commerciale :

Référence constructeur :

Version :

Description succincte :

Référence de l'agrément du moyen s'il a été soumis au ministère chargé des télécommunications :

C.2. Fabricant du moyen ou fournisseur de la prestation

Nom :

Raison sociale :

Adresse :

Numéro de téléphone :

Numéro de télécopie :

Adresse du courrier électronique :

C.3. Personne chargée du dossier technique

Nom et prénoms :

Adresse :

Numéro de téléphone :

Numéro de télécopie :

Adresse du courrier électronique :

C.4. Divers

Si le moyen ou la prestation utilise des moyens ou prestations préalablement déclarés ou autorisés, préciser, pour chacun d'eux, leur identification, référence et date de notification de déclaration ou d'autorisation :

ACTOBA

La lettre juridique des Médias et des réseaux de Communication

w w w . a c t o b a . c o m

C.5. Services de cryptologie fournis
Authentification (*) :

Contrôle d'accès (*) :

Signature (*) :

Intégrité (*) :

Confidentialité (*) :

Téléphone télécopie messagerie transmissions
de données (préciser le(s) type(s) de données
chiffrées, par exemple données à caractère
financier, médical, de gestion,...) :

Autre(s) (à préciser) (*) :

C.6. Installation des algorithmes Logiciel.

Matériel (à préciser) :

(*) Préciser le(s) nom(s) de(s) algorithme(s)
utilisé(s).

D. - Attestation Je soussigné (nom,
prénoms)..... agissant en qualité
de..... représentant le fournisseur -
exportateur - importateur - utilisateur (*) certifie
que les renseignements figurant sur cette
déclaration - demande d'autorisation (*) sont
exactes et ont été établis de bonne foi, toute
fausse déclaration ou tout manquement aux
engagements souscrits m'exposant aux
sanctions prévues par l'article 28 de la loi no 90-
1170 du 29 décembre 1990 modifiée et par le
décret no 98-101 du 24 février 1998.

Date :.....Signature :

(*) Rayer les mentions inutiles

PARTIE TECHNIQUE

A joindre au dossier de déclaration ou de
demande d'autorisation concernant les moyens
et prestations de cryptologie (1)

La partie technique comporte les informations
suivantes :

La référence commerciale du produit :

- nom

- numéro de la version

- la description générale du produit

- le manuel utilisateur

- la description des services offerts par le produit
;

- la description des fonctions de cryptologie
offertes par le produit (chiffrement, signature,
gestion de clés) ; soit la description complète
des procédés de cryptologie employés, sous la
forme d'une description mathématique et d'une
simulation dans un langage de haut niveau, type
C ou pascal. soit la référence à un dossier

préalablement déposé pour un produit usant du
même procédé de cryptologie, soit la référence
à un standard reconnu, non équivoque, et dont
les détails techniques sont accessibles aisément
et sans condition ;

- la description de la gestion des clés mises en
oeuvre par le moyen, incluant au moins : - le
mode de distribution ;

- le procédé de génération des clés ;

- le format de conservation des clés s'il y a lieu ;

- le format de transmission des clés s'il y a lieu ;

- la description des mesures techniques mises
en oeuvre pour empêcher l'altération du procédé
de chiffrement ou de la gestion de clés associée
(2) ;

- la description des prétraitements subis par les
données claires avant leur chiffrement
(compression, formatage, ajout d'un en-tête,
etc.)

- la description des post-traitements des
données chiffrées, après leur chiffrement (ajout
d'un en-tête, formatage, mise en paquet, etc.)

(1) Conformément au troisième alinéa de l'article
1er de l'arrêté ci-dessus, la partie technique doit
être accompagnée de deux exemplaires du
matériel concerné ou bien d'un exemplaire du
logiciel concerné;

(2) A fournir dans le cas d'une demande
d'autorisation seulement.