BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°13 du 16 mars 2012

TEXTE SIGNALE

ARRÊTÉ

définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie (à jour de ses 2 modificatifs : décret n° 2009-834 du 7 juillet 2009 (JO n° 156 du 8 juillet 2009, texte n° 3, signalé au BOC 4/2010/S1 et décret n° 2009-1657 du 24 décembre 2009 (JO n° 301 du 29 décembre 2009, texte n° 1, signalé au BOC 4/2010/S1).

Du *25 mai 2007*

SERVICE DES MOYENS GÉNÉRAUX.

ARRÊTÉ définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie (à jour de ses 2 modificatifs : décret n° 2009-834 du 7 juillet 2009 (JO n° 156 du 8 juillet 2009, texte n° 3, signalé au BOC 4/2010/S1 et décret n° 2009-1657 du 24 décembre 2009 (JO n° 301 du 29 décembre 2009, texte n° 1, signalé au BOC 4/2010/S1).

Du 25 mai 2007

NOR P R M D 0 7 5 3 6 6 9 A

Pièce(s) Jointe(s) :

Trois annexes.

Textes abrogés :

Arrêté du 13 mars 1998 (JO du 15, p. 3888 ; BOC, 2000, p. 12 ; BOEM 160.3).
Arrêté du 13 mars 1998 (JO du 15, p. 3888 BOC, 2000, p. 13 ; BOEM 160.3).
Arrêté du 13 mars 1998 (n.i. BO, JO du 15 mars 1998, p. 3888).
Arrêté du 13 mars 1998 (n.i. BO, JO du 15 mars 1998, p. 3891).
Arrêté du 13 mars 1998 (n.i. BO, JO du 15 mars 1998, p. 3891).
Arrêté du 17 mars 1999 (JO du 19, p. 4052 ; BOC, 2000, p. 19 ; BOEM 160.3).

Classement dans l'édition méthodique : BOEM 160.3

Référence de publication : JO n° 127 du 3 juin 2007, texte n° 1 ; signalé au BOC 13/2012.

Le Premier ministre,

Vu la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique ;

Vu le décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30., 31. et 36. de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie, notamment ses articles 4., 7. et 9.,

Arrête :

Art. 1er. La déclaration préalable prévue par l'article 3. du décret du 2 mai 2007 susvisé, en tant qu'elle est relative à une opération portant sur un moyen de cryptologie, est effectuée au moyen du formulaire joint en annexe I. (DM) au présent arrêté. Cette annexe précise les caractéristiques techniques qui peuvent être demandées au déclarant en vertu de l'article 7. du décret du 2 mai 2007 susvisé.

La déclaration préalable prévue par l'article 3. du décret du 2 mai 2007 susvisé, en tant qu'elle est relative à une fourniture de prestations de cryptologie, est effectuée au moyen du formulaire joint en annexe II. (DP) au présent arrêté.

Art. 2. La demande d'autorisation prévue par l'article 9. du décret du 2 mai 2007 susvisé est effectuée au moyen du formulaire joint en annexe III. (AM) au présent arrêté.

Art. 3. L'arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie, l'arrêté du 13 mars 1998 définissant

le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation, l'arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes, l'arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes, l'arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en œuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II. de l'article 28. de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications et l'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 sont abrogés.

Art. 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 25 mai 2007.

Pour le Premier ministre et par délégation :

Le secrétaire général de la défense nationale,

F. DELON.

ANNEXE I.

DÉCLARATION D'OPÉRATION RELATIVE À UN MOYEN DE CRYPTOLOGIE.

DÉCLARATION D'OPÉRATION RELATIVE À UN MOYEN DE CRYPTOLOGIE.

Formulaire [(1)] à adresser en trois exemplaires au secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information (bureau des relations industrielles), 51, boulevard de La Tour-Maubourg, 75700 Paris 07 SP (téléphone : 33 [0] 1-71-75-82-75, télécopie : 33 [0] 1-71-75-82-60).

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

Cocher la ou les cases correspondantes :

□ Déclaration de fourniture.

□ Déclaration de transfert depuis un État membre de la Communauté européenne.

□ Déclaration de transfert vers un État membre de la Communauté européenne.

□ Déclaration d'importation en provenance de :

□ Déclaration d'exportation.

[(1)] Formulaire disponible sur le site internet : http://www.ssi.gouv.fr/

A. Déclarant.

A-1. Société.

Joindre un document général présentant la société et un extrait K *bis* du registre du commerce et des sociétés datant de moins de trois mois (ou un document équivalent pour les sociétés de droit étranger) :

Dénomination sociale : ……...

Numéro SIRET :……..

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 : …….

A-2. Particulier.

Nom et prénoms : ……

Nationalité : …….

Adresse : ……..

Numéro de téléphone : ……

Numéro de télécopie : …….

Adresse du courrier électronique : ……..

B.-Moyen auquel s'applique la déclaration.

B-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) : ……

B-2. Fabricant du moyen de cryptologie (si différent du A-1).

Dénomination sociale : ……...

Numéro SIRET : …….

Nationalité : …….

Adresse : …….....

Numéro de téléphone : ……

Numéro de télécopie : …….

Adresse du courrier électronique : ……..

Adresse du site internet : …….

B-3. Personne chargée des caractéristiques techniques.

Nom et prénoms : ……

Nationalité : …….

Adresse : ……..

Numéro de téléphone : …….

Numéro de télécopie : …….

Adresse du courrier électronique : …….

B-4. Services de cryptologie fournis.

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

□ Authentification : ……..

□ Signature :……..

□ Contrôle d'intégrité :……..

□ Confidentialité : ……..

□ Autres (à préciser) : ……

B-5. Mise en œuvre des algorithmes.

□ Logiciel.

□ Matériel (à préciser) : ……

B-6. Normes ou standards de sécurité du moyen.

 Normes ou standards (à préciser) : ……..
……..

C. Cas d'un moyen de cryptologie relevant de la catégorie 3 de l'annexe 2 au décret n° 2007-663 du 2 mai 2007.

Présenter le mode de commercialisation du moyen de cryptologie : ……
…….

Expliquer pourquoi la fonctionnalité cryptographique ne peut pas être modifiée facilement par l'utilisateur : …….

Expliquer en quoi les modalités d'installation du moyen ne nécessitent pas d'assistance importante ultérieure de la part du fournisseur :
……..

D. Attestation.

Je soussigné (nom, prénoms) : …….

agissant en qualité de : ……

pour le compte de : ……..

représentant le " déclarant ", certifie que les renseignements figurant sur cette déclaration et joints à cette déclaration sont exacts et ont été établis de bonne foi, et que le déclarant s'engage à porter à la connaissance de l'Agence nationale de la sécurité des systèmes d'information, sans délai, tout élément nouveau de fait ou de droit de nature à modifier cette déclaration ou les éléments joints, toute omission ou toute fausse déclaration exposant le déclarant aux sanctions prévues aux articles 34. et 35. de la loi n° 2004-575 du 21 juin 2004 modifiée.

Date : …….

Signature

Caractéristiques techniques à fournir sur demande de la direction centrale de la sécurité des systèmes d'information.

(À fournir en trois exemplaires [sauf pour les éléments visés au point 1])

1. Les éléments nécessaires pour mettre en œuvre le moyen de cryptologie :

a) Deux modèles du moyen de cryptologie ;

b) Les guides d'installation du moyen ;

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, 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 mode de distribution des clés ;

b) Le procédé de génération des clés ;

c) Le format de conservation des clés ;

d) Le format de transmission 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 :

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 stockés les fonctions et les paramètres de cryptologie ainsi que les références de ces mémoires.

ANNEXE II.

DÉCLARATION DE FOURNITURE D'UNE PRESTATION DE CRYPTOLOGIE.

DÉCLARATION DE FOURNITURE D'UNE PRESTATION DE CRYPTOLOGIE.

Formulaire [(1)] à adresser en trois exemplaires au secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information (bureau des relations industrielles), 51, boulevard de La Tour-Maubourg, 75700 Paris 07 SP (téléphone : 33 [0] 1-71-75-82-75, télécopie : 33 [0] 1-71-75-82-60).

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

Déclaration.

☐ Si la prestation consiste en la délivrance de certificats électroniques qualifiés au sens du décret n° 2001-272 du 30 mars 2001 modifié, cocher la case.

[(1)] Formulaire disponible sur le site internet : http://www.ssi.gouv.fr/

A. Déclarant.

A-1. Société.

Joindre un document général présentant la société et un extrait K *bis* du registre du commerce et des sociétés datant de moins de trois mois (ou un document équivalent pour les sociétés de droit étranger) :

Dénomination sociale : ……

Numéro SIRET :……

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 : ……..

A-2. Particulier.

Nom et prénoms : …….

Nationalité : …….

Adresse : ……...

Numéro de téléphone : …….

Numéro de télécopie : …….

Adresse du courrier électronique : ……..

B. Description de la prestation.

B-1. Catégories d'utilisateurs auxquels est destinée la prestation.

□ Administrations (à préciser) :…….
……

□ Grandes entreprises (préciser le secteur d'activité) :……..
……

□ Établissements financiers :…….
…….....

□ PME (préciser le secteur d'activité) :……..
…….

□ Professions libérales (préciser le secteur d'activité) :……
……...

□ Autres (à préciser avec le secteur d'activité) : …….

B-2. Types de données concernées par la prestation.

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

B-3. Services de cryptologie fournis.

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

□ Authentification :……...

□ Signature :……..

□ Confidentialité :…….

□ Horodatage :……..

□ Archivage sécurisé :……..

□Gestion de clés cryptographiques :……

□Certification de clés ou de données :…….

□Autres (à préciser) : ……...

B-4. Personne chargée des éléments techniques.

Nom et prénoms : …….

Nationalité : …….

Adresse : ……...

Numéro de téléphone : …….

Numéro de télécopie : ……..

Adresse du courrier électronique : ……

C. Moyens de cryptologie mis en œuvre par le prestataire.

Pour les moyens de cryptologie mis en œuvre par le prestataire pour fournir sa prestation, indiquer :

Référence commerciale des moyens : ……..

Référence constructeur des moyens : ……..

Version : ……..

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

…….

D. Attestation.

Je soussigné (nom, prénoms) : ……

agissant en qualité de : ……

pour le compte de : ……

représentant le " déclarant ", certifie que les renseignements figurant sur cette déclaration et joints à cette déclaration sont exacts et ont été établis de bonne foi, et que le déclarant s'engage à porter à la connaissance de l'Agence nationale de la sécurité des systèmes d'information, sans délai, tout élément nouveau de fait ou de droit de nature à modifier cette déclaration ou les éléments joints, toute omission ou toute fausse déclaration exposant le déclarant aux sanctions prévues aux articles 34. et 35. de la loi n° 2004-575 du 21 juin 2004 modifiée et à l'article 13. du décret n° 2007-663 du 2 mai 2007.

Date : ……

Signature

Éléments techniques à joindre obligatoirement à la déclaration de fourniture d'une prestation de cryptologie.

(À joindre en trois exemplaires).

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 des 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 de clés cryptographiques ou de certificats électroniques au profit des utilisateurs :

a) La description de la procédure de génération des clés et des certificats ;

b) La description de la procédure de distribution et de remise des clés et des certificats aux utilisateurs ;

c) La description des mesures techniques et organisationnelles mises en œuvre pour la protection et la conservation des clés ;

d) La description de la procédure de recouvrement des clés (uniquement pour le service de 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 clés ou les certificats délivrés par ce prestataire.

ANNEXE III.

DEMANDE D'AUTORISATION OU DE RENOUVELLEMENT D'AUTORISATION D'OPÉRATION RELATIVE À UN MOYEN DE CRYPTOLOGIE.

DEMANDE D'AUTORISATION OU DE RENOUVELLEMENT D'AUTORISATION D'OPÉRATION RELATIVE À UN MOYEN DE CRYPTOLOGIE.

Formulaire [1] à adresser en trois exemplaires au secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information (bureau des relations industrielles), 51, boulevard de La Tour-Maubourg, 75700 Paris 07 SP (téléphone : 33 [0] 1-71-75-82-75, télécopie : 33 [0] 1-71-75-82-60).

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

Cocher la ou les cases correspondantes :

☐ Demande d'autorisation de transfert vers un État membre de la Communauté européenne pour une durée de…….. (cinq ans au maximum).

☐ Demande d'autorisation d'exportation vers un État n'appartenant pas à la Communauté européenne pour une durée de…….. (cinq ans au maximum).

☐ Demande de renouvellement d'une autorisation de transfert pour une durée de..... (cinq ans au maximum).

☐ Demande de renouvellement d'une autorisation d'exportation pour une durée de..... (cinq ans au maximum).

[1] Formulaire disponible sur le site internet : http://www.ssi.gouv.fr/

A. Demandeur d'autorisation.

A-1. Société.

Joindre un document général présentant la société et un extrait K *bis* du registre du commerce et des sociétés datant de moins de trois mois (ou un document équivalent pour les sociétés de droit étranger) :

Dénomination sociale : …….

Numéro SIRET : ……..

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 : ……

A-2. Particulier.

Nom et prénoms : …….

Nationalité : ……..

Adresse : ……..
……..

Numéro de téléphone : …….

Numéro de télécopie : ……...

Adresse du courrier électronique : ……

B. Moyen auquel s'applique la demande d'autorisation

B-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) :

B-2. Fabricant du moyen de cryptologie (si différent du A-1).

Dénomination sociale : …….

Numéro SIRET : ……..

Nationalité : ……..

Adresse : ……...
……..

Numéro de téléphone : …….

Numéro de télécopie : ……..

Adresse du courrier électronique : ……

Adresse du site internet : …….

B-3. Personne chargée des éléments techniques.

Nom et prénoms : …….

Nationalité : ……..

Adresse : ……..
……..

Numéro de téléphone : …….

Numéro de télécopie : ……..

Adresse du courrier électronique : ……

B-4. Services de cryptologie fournis.

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

□ Authentification :……...

□ Signature :…….

□ Contrôle d'intégrité :…….

□ Confidentialité :……

□ Autres (à préciser) : ……

B-5. Mise en œuvre des algorithmes.

□ Logiciel.

□ Matériel (à préciser) : ……...

B-6. Normes ou standards de sécurité du moyen.

□ Normes ou standards (à préciser) : ……...
……...

C. Renouvellement d'autorisation de transfert ou d'exportation.

Si le moyen de cryptologie, avec les mêmes éléments techniques, a déjà été l'objet d'une autorisation de transfert ou d'exportation, indiquer les références de cette autorisation :

Numéro de dossier (mentionné sur le récépissé et sur l'autorisation) : ……

Date de l'autorisation : ……..

Numéro de l'autorisation (mentionné sur l'autorisation) : ……

D. Attestation.

Je soussigné (nom, prénoms) : ……

agissant en qualité de : ……

pour le compte de : …….

représentant le " demandeur d'autorisation ", certifie que les renseignements figurant sur cette demande d'autorisation et joints à cette demande sont exacts et ont été établis de bonne foi, et que le demandeur s'engage à porter à la connaissance de l'Agence nationale de la sécurité des systèmes d'information, 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 34. et 35. de la loi n° 2004-575 du 21 juin 2004 modifiée.

Date : …….

Signature

Éléments techniques à joindre obligatoirement à la demande d'autorisation d'une opération relative à un moyen de cryptologie.

(À joindre en trois exemplaires
[sauf pour les éléments visés au point 1]).

1. Les éléments nécessaires pour mettre en œuvre le moyen de cryptologie (à ne fournir que sur demande de l'Agence nationale de la sécurité des systèmes d'information) :

a) Deux modèles du moyen de cryptologie ;

b) Les guides d'installation du moyen ;

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, 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 mode de distribution des clés ;

b) Le procédé de génération des clés ;

c) Le format de conservation des clés ;

d) Le format de transmission 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 l'Agence nationale de la sécurité des systèmes d'information) :

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 stockés les fonctions et les paramètres de cryptologie ainsi que les références de ces mémoires.