

ANNEXE I

DÉCLARATION ET DEMANDE D'AUTORISATION D'OPÉRATIONS RELATIVES A UN MOYEN DE CRYPTOLOGIE

FORMULAIRE¹ à adresser en deux exemplaires à :

Agence nationale de la sécurité des systèmes d'information
Bureau des contrôles réglementaires
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP
(Téléphone : + 33 (0)1 71 75 82 75 ; Mél : controle@ssi.gouv.fr)

Le présent formulaire permet d'effectuer les formalités prévues aux chapitres II et III du décret n° 2007-663 du 2 mai 2007 pour les opérations suivantes relatives à un moyen de cryptologie :

- la déclaration de fourniture, de transfert depuis ou vers un État membre de l'Union européenne, d'importation et d'exportation² vers un État n'appartenant pas à l'Union européenne ;
- la demande d'autorisation ou de renouvellement d'autorisation de transfert vers un État membre de l'Union européenne et d'exportation vers un État n'appartenant pas à l'Union européenne.

Cochez la case correspondant aux formalités que vous souhaitez effectuer :

- ☐ **déclaration et demande d'autorisation de toute opération relative à un moyen de cryptologie.**

En cochant cette case, vous effectuez les formalités relatives à toutes les opérations de fourniture, de transfert depuis ou vers un État membre de l'Union européenne, d'importation et d'exportation hors de l'Union européenne d'un moyen de cryptologie relevant des chapitres II et III du décret n° 2007-663 du 2 mai 2007.

- ☐ **déclaration de fourniture, de transfert depuis ou vers un État membre de l'Union européenne, d'importation et d'exportation vers un Etat n'appartenant pas à l'Union européenne d'un moyen de cryptologie.**

En cochant cette case, vous effectuez les formalités relatives aux seules opérations relevant du chapitre II du décret n° 2007-663 du 2 mai 2007.

- ☐ **demande d'autorisation de transfert vers un État membre de l'Union européenne et d'exportation vers un Etat n'appartenant pas à l'Union européenne d'un moyen de cryptologie.**

En cochant cette case, vous effectuez les formalités relatives aux seules opérations relevant du chapitre III du décret n° 2007-663 du 2 mai 2007.

- ☐ **demande de renouvellement d'autorisation de transfert vers un État membre de l'Union européenne et d'exportation d'un moyen de cryptologie.**

Voir paragraphe D du formulaire.

¹ Le formulaire est disponible sur le site internet www.ssi.gouv.fr.

² La déclaration d'exportation ne s'applique qu'aux opérations d'exportation prévues à l'annexe 2 du décret n° 2007-663 du 2 mai 2007.

A. – Déclarant et/ou demandeur

Le « déclarant et/ou demandeur » désigne ci-après la personne effectuant la déclaration et/ou la demande d'autorisation d'opération relative à un moyen de cryptologie.

A.1. Personne morale

Paragraphe à remplir lorsque le déclarant et/ou le demandeur est une personne morale (société, administration, association, etc.).

Dénomination sociale :
Numéro SIRET :
Nationalité :
Adresse :
.....
Numéro de téléphone :

Personne chargée du dossier administratif

Nom et prénoms :
Adresse :
.....
Numéro de téléphone :
Adresse de courrier électronique :

Personne chargée des éléments techniques

Nom et prénoms :
Adresse :
.....
Numéro de téléphone :
Adresse de courrier électronique :

A.2. Personne physique

Paragraphe à remplir lorsque le déclarant et/ou le demandeur est une personne physique (particulier).

Nom et prénoms : **PICARD VINCENT**
Nationalité : **FRANCAISE**
Adresse : **Le Barbois 14240 SALLEN**
.....
Numéro de téléphone : **06 61 70 77 22**
Adresse de courrier électronique : **v.picard1976@gmail.com**

**B. – Moyen de cryptologie auquel s'appliquent la déclaration
et/ou la demande d'autorisation**

B.1. Informations générales sur le moyen

Désignation générique du moyen (selon le format [MARQUE DE DISTRIBUTION – DENOMINATION DU MOYEN]) :

Version :

Référence commerciale :

Date de mise sur le marché :

Si le déclarant et/ou le demandeur n'est pas le fabricant du moyen de cryptologie, précisez les éléments suivants :

Fabricant : Apple / iOS

Dénomination d'origine du moyen :

B.2. Description fonctionnelle du moyen

B.2.1. Classez le moyen dans la ou les catégorie(s) correspondante(s) :

☐ Matériel

☒ Logiciel

B.2.2. Description générale du moyen :

Utilisation du HTTPS standard fournie par Apple.

.....
.....
.....
.....
.....

B.2.3. Indiquez à quelle catégorie se rapporte la fonction principale du moyen :

☒ Sécurité de l'information (moyen de chiffrement, bibliothèque cryptographique, etc.)

☐ Ordinateur (système d'exploitation, serveur, logiciel de virtualisation, etc.)

☐ Envoi, stockage, réception d'informations (terminal de communication, logiciel de gestion, etc.)

☐ Réseau (logiciel de supervision, routeur, station de base, etc.)

☐ Autres. Si oui, précisez :

B.3. Description technique des services de cryptologie fournis

B.3.1. Description des fonctionnalités cryptographiques du moyen :

.....
.....
.....
.....
.....

B.3.2. Indiquez à quelle(s) catégorie(s) se rapporte(nt) la ou les fonctions cryptographiques du moyen :

- ☒ Authentification
- ☐ Intégrité
- ☐ Confidentialité
- ☐ Signature

B.3.3. Indiquez le(s) protocole(s) sécurisé(s) utilisés par le moyen :

- ☐ IPsec
- ☐ SSH
- ☒ SSL/TLS
- ☐ Protocoles liés à la VoIP (de type SIP/RTP)
- ☐ Autres. Si oui, précisez :

B.3.4. Précisez les algorithmes cryptographiques utilisés et leurs longueurs maximales de clés :

Algorithme	Mode	Taille de clé associée	Fonction

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

- ☐ *En cochant cette case, vous déclarez que le moyen de cryptologie relève de la catégorie 3 de l'annexe 2 du décret n° 2007-663 du 2 mai 2007. Dans ce cas, renseignez les éléments justificatifs ci-après :*

- Présentez le mode de commercialisation du moyen de cryptologie et le marché auquel il s'adresse :
[Gratuit et fourni par Apple sur iOS](#)
.....
.....

- Expliquez pourquoi la fonctionnalité cryptographique du moyen ne peut pas être modifiée facilement par l'utilisateur :

.....

.....

.....

.....

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

.....

.....

.....

.....

D. – Renouvellement d'autorisation de transfert ou d'exportation

Lorsque le moyen de cryptologie a déjà été l'objet d'une autorisation de transfert ou d'exportation, indiquez 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) :

E. – Pièces à joindre (cochez les cases correspondant aux pièces que vous avez jointes)

- | | |
|---|--------------------------|
| - document général présentant la société (<i>format électronique souhaité</i>) | <input type="checkbox"/> |
| - 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) | <input type="checkbox"/> |
| - brochure commerciale du moyen de cryptologie (<i>format électronique souhaité</i>) | <input type="checkbox"/> |
| - brochure technique du moyen de cryptologie (<i>format électronique souhaité</i>) | <input type="checkbox"/> |
| - manuel utilisateur (si disponible) (<i>format électronique souhaité</i>) | <input type="checkbox"/> |
| - guide administrateur (si disponible) (<i>format électronique souhaité</i>) | <input type="checkbox"/> |

F. – Attestation

Je soussigné (nom, prénoms) : PICARD Vincent

agissant en qualité de :

pour le compte de :

représentant le déclarant et/ou le demandeur, certifie que les renseignements figurant sur ce formulaire et les pièces qui lui sont jointes sont exacts et ont été établis de bonne foi et que le déclarant et/ou 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 déclaration et/ou cette demande d'autorisation ou les éléments joints, toute omission ou toute fausse déclaration exposant le déclarant et/ou le demandeur aux sanctions prévues aux articles 34 et 35 de la loi n° 2004-575 du 21 juin 2004 modifiée.

Date : 18/05/2022

Signature



ELÉMENTS ET CARACTÉRISTIQUES TECHNIQUES À COMMUNIQUER
SUR DEMANDE DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES
SYSTÈMES D'INFORMATION

(A fournir de préférence au format électronique)

1. Les éléments nécessaires pour mettre en œuvre le moyen de cryptologie :
 - a) deux exemplaires 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 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.
3. 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.
4. Les éléments relatifs à la conception du moyen 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 stockés les fonctions et les paramètres de cryptologie ainsi que les références de ces mémoires.

