ANNEXE II

DÉCLARATION DE FOURNITURE D'UNE PRESTATION DE CRYPTOLOGIE

FORMULAIRE[1] 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 ; Mèl : controle@ssi.gouv.fr)

❑ Si la prestation consiste à délivrer des certificats électroniques qualifiés au sens du décret n° 2001-272 du 30 mars 2001 modifié, cochez la case.

A. – Déclarant

A-1. Personne morale

Dénomination sociale : T-Shaped Innovatie B.V.
Numéro SIRET : Not available (Dutch registration ID : #####)
Nationalité : PAYS BAS
Adresse : ###STREET NR CITY### PAYS BAS
Numéro de téléphone : +31 ######

Personne chargée du dossier administratif :
Nom et prénoms : VAN DER VORST, Tommy
Adresse : ###STREET NR CITY### PAYS BAS
Numéro de téléphone : +31 ######
Adresse du courrier électronique : ###MAIL

~~*A-2. Particulier*~~

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

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

B. – Description de la prestation

Dénomination de la prestation : Synctrain, Syncthing for iOS/macOS

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

- ❑ Administrations (précisez lesquelles) : ____ ❑ Grandes entreprises (précisez le secteur d'activité) : __ ❑ Etablissements financiers : __ ❑ PME (précisez le secteur d'activité) : __ ❑ Professions libérales (précisez le secteur d'activité) : _____
- ❑ Autres (précisez le secteur d'activité) : ____

Tout utilisateur d'appareil Apple souhaitant synchroniser des fichiers entre appareils.

B-2. Types de données concernées par la prestation

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

Toutes les données (fichiers) que l'utilisateur de l'application décide d'utiliser.

B-3. Services de cryptologie fournis

Précisez 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 (précisez) :___

En transit :

- QUIC/TLS 1.2/TLS 1.3 (connexions périphérique à appareil, authentification et chiffrement en transit). La cryptographie TLS standard est utilisée (par exemple ECDH/ECDSA/RSA/SHA), voir ici pour l'ensemble de chiffrement configuré en cours de configuration.
- SHA-256 (certificate fingerprints / 'device IDs')

Chiffrement des fichiers au repos (« chiffrement de périphérique non fiable ») :

- Scrypt (folder key derivation)
- AES-SIV-256 (file name encryption). AEAD scheme based on AES-128 (32 byte keys)
- HKDF + SHA256 (per-file key derivation)
- XChaCha20-Poly1305 (file contents and metadata encryption)

B-4. Personne chargée des éléments techniques

Nom et prénoms : VAN DER VORST, Tommy
Adresse : ###STREET NR CITY### PAYS BAS

Numéro de téléphone : +31 ######
Adresse du courrier électronique : ###MAIL###

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, indiquez :

Désignation générique du moyen (*selon le format « MARQUE DE DISTRIBUTION – DENOMINATION DU MOYEN ») :* _____
Version :_____ Référence commerciale : ___
Le cas échéant, référence des déclarations ou des autorisations relatives aux moyens : _____
_____

Comme expliqué ci-dessus, T-Shaped lui-même ne fournit pas de service aux utilisateurs finaux pour faciliter le partage de fichiers. Les appareils fonctionnant sous Synctrain ou des logiciels compatibles Syncthing se connectent directement ou utilisent des services proposés par des tiers (principalement la Syncthing Foundation). T-Shaped n'est pas associée à la Syncthing Foundation.

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

- document général présentant la société *(format électronique souhaité)* ❑

Veuillez voir ci-dessous.

- 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) ❑

Un certificat d'enregistrement auprès de la Chambre de commerce néerlandaise est joint.

E. – Attestation

Je soussigné (nom, prénoms) : VAN DER VORST, Tommy agissant en qualité de :

Director pour le compte de : T-Shaped Innovatie B.V.

représentant le déclarant, certifie que les renseignements figurant sur cette déclaration et les pièces qui lui sont jointes 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

ELÉMENTS TECHNIQUES À JOINDRE OBLIGATOIREMENT À LA DÉCLARATION DE FOURNITURE D'UNE PRESTATION DE CRYPTOLOGIE

(A fournir de préférence au format électronique)

1. La description des services offerts aux utilisateurs de la prestation.

Synctrain est une application qui permet une synchronisation chiffrée de bout en bout directement entre les appareils de l'utilisateur. L'application est conçue pour les appareils Apple et fonctionne actuellement sur iOS et macOS.

Synctrain est construit autour de Syncthing, une solution logicielle open source pour la synchronisation de fichiers, qui fonctionne sur de nombreuses plateformes différentes (y compris Windows, Linux et macOS). Synctrain peut synchroniser des fichiers avec d'autres appareils qui exécutent Synctrain, Syncthing ou d'autres logiciels compatibles Syncthing. Syncthing est développé par des développeurs open source indépendants (« The Syncthing Authors »). La Fondation Syncthing en soutient le développement. T-Shaped n'est pas associée à la fondation Syncthing.

Comme la bibliothèque Syncthing est écrite en Go, elle n'utilise pas les primitives cryptographiques fournies par le système d'exploitation Apple, mais plutôt celles proposées par la bibliothèque standard Go et les packages (et donc incluses dans l'application).

La communication entre les appareils (« en transit ») est chiffrée à l'aide de protocoles standards de l'industrie (QUIC/TLS). Au premier démarrage, chaque appareil génère une clé privée et un certificat associé. L'appareil présente un hachage du certificat (« ID de l'appareil ») à l'utilisateur. L'utilisateur peut alors configurer chaque appareil pour permettre des connexions depuis et vers certains identifiants d'appareil. Lors de la connexion, la vérification d'identité s'effectue sur la base des certificats. De plus, les appareils utilisent l'identifiant d'appareil pour s'annoncer auprès d'autres appareils et pour retrouver d'autres appareils sur le réseau local et sur Internet.

En option, Synctrain/Syncthing peut chiffrer les fichiers de manière à ce que l'appareil récepteur ne puisse *pas les déchiffrer*. De cette façon, l'appareil distant peut être utilisé pour stocker un fichier sur un appareil distant qui pourra être téléchargé ultérieurement par l'appareil qui l'a mis là, ou par tout autre appareil possédant la clé de chiffrement. La clé de chiffrement est dérivée d'un mot de passe de dossier configurable par l'utilisateur.

Synctrain **ne nécessite pas** un fournisseur de services central pour faciliter la synchronisation des fichiers. T-Shaped ne fournit que l'application et aucun service facilitant son fonctionnement. Syncthing et Synctrain peuvent **en option** utiliser les services centralisés suivants, fournis par des tiers :

1. Découverte : cela permet aux appareils de se retrouver lorsqu'ils tentent de se connecter via Internet ;
2. STUN: cela permet aux appareils de trouver leur propre adresse internet lorsqu'ils tentent de se connecter sur Internet ;

3. Relais : cela permet aux appareils de communiquer entre eux, lorsque l'un ou les deux appareils sont derrière un pare-feu qui limite la connectivité internet ;
4. Pool relais : cela permet aux appareils de trouver un serveur relais à utiliser ;
5. Rapport d'utilisation : cela permet à l'application de rapporter des statistiques aux développeurs Syncthing sur l'utilisation de l'application.

Au premier démarrage, l'utilisateur est proposé d'utiliser les services mentionnés ci-dessus tels que fournis par la Syncthing Foundation. Alternativement, l'utilisateur peut choisir de ne pas utiliser les services centralisés ou de configurer les siens.

Les protocoles et formats de données utilisés sont spécifiés publiquement à https://docs.syncthing.net/specs/index.html.

Le code source complet de Synctrain est disponible ici : https://github.com/pixelspark/sushitrain (Sushitrain est le nom du projet open source, tandis que Synctrain est la version publiée par T-Shaped).

Le code source complet de Syncthing est disponible ici : https://github.com/syncthing/syncthing

2. La description des fonctions cryptologiques mises en œuvre par le prestataire.

1. Chiffrement en transit des communications (fichiers et métadonnées de fichiers) pour la synchronisation directe des fichiers entre appareils
2. Chiffrement en transit des communications (fichiers et métadonnées de fichiers) pour la synchronisation des fichiers entre appareils, médié par des services tiers.
3. Chiffrement optionnel au repos des fichiers et métadonnées avant l'envoi vers d'autres appareils (« chiffrement par pairs non fiable »).

3. La description des locaux utilisés pour mettre en œuvre la prestation.

Synctrain s'exécute sur l'appareil ou les appareils de l'utilisateur. T-Shaped ne fournit pas les services nécessaires au fonctionnement de l'application.

L'application Synctrain est principalement distribuée via le service Apple App Store.

Synctrain peut éventuellement utiliser des services tiers (comme décrit ci-dessus) à son choix. Les services proposés par la Fondation Syncthing sont couramment utilisés. Ces derniers sont (actuellement) fournis par des centres de données en Europe (Allemagne, France, Finlande actuellement).

4. La description des matériels et des logiciels informatiques et notamment des moyens de cryptologie utilisés par le prestataire.

La cryptographie contenue dans Synctrain est implémentée dans la bibliothèque standard (étendue) du langage de programmation Go ainsi que dans plusieurs paquets Go open source. L'application peut également (indirectement) s'appuyer sur la cryptographie fournie par le système d'exploitation (iOS/macOS).

5. La description des systèmes de protection physique et de contrôle d'accès aux locaux et aux systèmes informatiques du prestataire.

Comme décrit, aucun service fourni par T-Shaped n'est nécessaire au fonctionnement de l'application Synctrain.

Des mesures de sécurité opérationnelle sont appliquées pour protéger, par exemple, le code source et le compte de publication (App Store).

6. Lorsque la prestation consiste en la gestion de clés cryptographiques ou de certificats électroniques au profit des utilisateurs :

Comme discuté, T-Shaped ne fournit pas de service de gestion de certificats ou de clés pour les utilisateurs. L'application elle-même fournit cependant des certificats/clés. Pour plus de complétude, cela est décrit ci-dessous.

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

Les appareils génèrent leur propre clé privée et certificat lors du premier démarrage (ou se régénèrent à la demande explicite de l'utilisateur). Ces clés sont ensuite enregistrées sur le disque de l'appareil.

Alternativement, les utilisateurs peuvent générer et fournir leur propre clé/certificat à utiliser par l'application, en le plaçant à un emplacement précis sur le disque.

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

La clé privée ne quitte normalement jamais l'appareil (l'utilisateur peut cependant l'extraire manuellement, la migrer vers un autre appareil, etc.).

Le certificat est présenté aux autres appareils à chaque connexion dans le cadre du mécanisme d'authentification (authentification mutuelle standard TLS/QUIC).

L'utilisateur se voit montrer un identifiant de périphérique calculé comme une empreinte digitale de certificat (hash). L'ID de l'appareil sert à identifier les appareils et à vérifier le chiffrement de bout en bout.

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

L'application sauvegarde la clé privée localement sur l'appareil. L'application applique des classes de protection des données telles que le fichier ne peut être lu que lorsque l'appareil n'est pas déverrouillé par l'utilisateur. Sur macOS, la clé est accessible à l'utilisateur une fois connecté. Sur iOS, la clé est accessible en effectuant une sauvegarde de l'appareil.

d) La description de la procédure de recouvrement des clés (uniquement pour le service de confidentialité) ;

L'application ne fournit pas de mécanisme pour la récupération des clés. Lorsqu'une clé privée est perdue, l'appareil ne pourra pas s'authentifier auprès d'autres appareils. Pour résoudre cette situation,

une nouvelle clé doit être générée, et l'identifiant correspondant de l'appareil (empreinte digitale du certificat) doit être configuré sur les autres appareils.

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.

Présentation générale de la compagnie

L'application open source Synctrain a été développée par Tommy van der Vorst, avec la contribution d'autres personnes. Le projet open source s'appelle « Sushitrain ». Le code est sous licence Mozilla Public License 2.0 (MPL 2.0).

T-Shaped Innovatie BV agit en tant que *éditeur* de cette application sur l'App Store d'Apple. L'application publiée est fournie gratuitement et est conçue sans modifications du code open source. Le nom et le logo Synctrain appartiennent à T-Shaped et ne sont pas sous licence MPL 2.0 pour prévenir la fraude et les abus.

T-Shaped est une entreprise néerlandaise à responsabilité limitée. Il n'a qu'un seul réalisateur et propriétaire (Tommy van der Vorst). T-Shaped fournit des services de recherche et de conseil dans le domaine de l'innovation, notamment liés aux télécommunications, à la politique d'innovation et au développement logiciel.

Synctrain est construit autour de Syncthing, une solution open source pour la synchronisation des fichiers. Le projet Syncthing a été lancé par Jakob Borg et est actuellement maintenu par une communauté de contributeurs indépendants open source.

Des services complémentaires pour Syncthing sont fournis par la Syncthing Foundation, enregistrée en Suède. T-Shaped n'est pas affilié à la Syncthing Foundation. Synctrain n'est pas approuvé par la Syncthing Foundation ni par les auteurs de Syncthing.