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) : ____

Any Apple device user that wants to synchronize files between devices.

B-2. Types de données concernées par la prestation

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

Any data (files) that the user of the app decides to use.

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) :___

In-transit:

- QUIC/TLS 1.2/TLS 1.3 (device-to-device connections, authentication and in-transit encryption). Standard TLS cryptography is used (e.g. ECDH/ECDSA/RSA/SHA), see here for the current cipher set configured.
-
- SHA-256 (certificate fingerprints / ‘device IDs’)

File encryption at-rest (‘untrusted device encryption’) :

- 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 : _____
_____

As explained above, T-Shaped itself does not provide a service to end users to facilitate file sharing. Devices running Synctrain or Syncthing(-compatible) software connect directly or using services offered by third parties (primarily the Syncthing Foundation).

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

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

Please see below.

- 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) ❑

A certificate of registration with the Dutch Chamber of Commerce is attached.

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 is an app that provides end-to-end encrypted file synchronisation directly between the user's devices. The app is designed for Apple devices, and currently runs on iOS and macOS. Synctrain is built around Syncthing, an open source software solution for file synchronization, that works on many different platforms (including Windows, Linux and macOS). Synctrain can synchronize files with other devices that run Synctrain, Syncthing, or other Syncthing-compatible software.

As the Syncthing library is written in Go, it does not use the cryptography primitives provided by the Apple operating system, but rather those offered by the Go standard library and packages (and hence included in the app).

The communication between devices ('in-transit') is encrypted using industry standard protocols (QUIC/TLS). Upon first startup, each device generates a private key and associated certificate. The device presents a hash of the certificate ('device ID') to the user. The user can then configure each device to allow connections from and to certain device IDs. When connecting, identity verification takes place based on the certificates. Additionally, the devices use the device ID to announce themselves to other devices and to find other devices on the local network and the internet.

Optionally, Synctrain/Syncthing can encrypt files such that the receiving device cannot *decrypt* them. This way, the remote device can be used to store a file on a remote device that can be downloaded at a later time by the device that put it there, or any other device, that posesses the encryption key. The encryption key is derived from a user-configurable folder password.

Synctrain does **not** require a central service provider to facilitate file synchronization. T-Shaped only provides the application and no services that facilitate the app's functioning. Syncthing and Synctrain can **optionally** make use of the following centralized services, provided by third parties:

- Discovery : this allows devices to find each other when attempting to connect over the internet;
- STUN : this allows devices to find out their own internet address when attempting to connect over the internet ;
- Relaying : this allows devices to communicate with each other, when one or both devices are behind a firewall that restricts internet connectivity ;
- Relaying pool : this allows devices to find a relaying server to use ;
- Usage reporting : this allows the app to report statistics to the Syncthing developers on the app's usage.

On first startup, the user is offered to use the above services provided by the Syncthing Foundation. Alternatively the user can choose not to use the centralized services, or configure their own.

The protocols and data formats used are specified publicly at https://docs.syncthing.net/specs/index.html.

The full source code for Synctrain is available here : https://github.com/pixelspark/sushitrain (Sushitrain is the name of the open source project, whereas Synctrain is the published version by T-Shaped. In the future, we may make the app available as 'Syncthing for iOS').

The full source code for Syncthing is available here : https://github.com/syncthing/syncthing

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

- In-transit encryption of communication (files and file metadata) for file synchronization directly between devices
- In-transit encryption of communication (files and file metadata) for file synchronization between devices, mediated by third-party services.
- Optional at-rest encryption of files and metadata before sending to other devices ('untrusted peer encryption').

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

Synctrain runs on the user's device(s). T-Shaped does not provide services required for the app to function.

The Synctrain app is primarily distributed through the Apple App Store service.

Synctrain can optionally make use of third-party services (as described above) at the user's choice. The services offered by the Syncthing Foundation are commonly used. These are (currently) provided from datacenters within Europe (Germany, France, Finland currently).

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

The cryptography contained in Synctrain is implemented in the standard library of the Go programming language as well as several open source Go packages. The app may also (indirectly) rely on the cryptography provided by the operating system (iOS/macOS).

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

As described there are no services provided by T-Shaped that are required for the functioning of the Synctrain app.

Operational security measures are applied to protect e.g. the source code and (App Store) publishing account.

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

As discussed, T-Shaped does not provide a service for certificate or key management for users. The app itself however provides certificates/keys. For completeness this is described below.

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

Devices generate their own private key and certificate upon first start-up (or re-generate at the expliciet request of the user). These keys are then saved to disk on the device.

Alternatively, users can generate and supply their own key/certificate for the app to use, by placing it in a specific location on disk.

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

The private key normally never leaves the device (the user can however manually extract it, migrate it to another device, etc.).

The certificate is presented to other devices upon each connection as part of the authentication mechanism (standard TLS/QUIC mutual authentication).

The user is shown a device ID which is calculated as a certificate fingerprint (hash). The device ID is used for identifying devices and verifying end-to-end encryption.

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

The app saves the private key locally on the device. The app applies data protection classes such that the file cannot be read until the device is first unlocked by the user. On macOS, the key is accessible by the user once logged in. On iOS, the key is accessible by performing a device back-up.

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

The app does not provide a mechanism for key recovery. When a private key is lost, the device will be unable to authenticate to other devices. To resolve this situation, a new key needs to be generated, and the corresponding device ID (certificate fingerprint) must be configured on the other devices.

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.

General company presentation

The Synctrain open source app was developed by Tommy van der Vorst, with contributions by others. The open source project is called ‘Sushitrain’. The code is licensed under the Mozilla Public License 2.0 (MPL 2.0).

T-Shaped Innovatie B.V. (« T-Shaped ») acts as the *publisher* of this app on the Apple App Store. The published app is provided free of charge and is built without changes from the open source code. The

Synctrain name and logo are owned by T-Shaped and not MPL 2.0 licensed to prevent fraud and misuse.

T-Shaped is a Dutch company with limited liability. It has a single director and owner (Tommy van der Vorst). T-Shaped provides research and consultancy services in the area of innovation, specifically related to telecommunications, innovation policy and software development.

Synctrain is built around Syncthing, an open source solution for file synchronization. The Syncthing project was started by Jakob Borg, and is currently maintained by a community of open source contributors.

Supplementary services for Syncthing are provided by the Syncthing Foundation, which is registered in Sweden. Syncthing