Epsitec SA Rue de Neuchâtel 32 info@cresus.ch
1400 Yverdon-les-Bains www.cresus.ch

Crésus Synchro – détails techniques

Composants installés

Le service Crésus Synchro s'installe séparément pour chaque utilisateur Windows :

- Le programme, les binaires et ses ressources se trouvent dans `%localappdata%\cresus_synchro`
- Les réglages et clés des mandats sont stockés dans `%localappdata%\Epsitec\Cresus Synchro`
- Des fichiers temporaires sont stockés à côté des fichiers Crésus dans un dossier caché `.crsync`.

Canaux de communication

Crésus Synchro utilise trois canaux de communication :

- Directement avec les modules Crésus installés sur la même machine (via des sockets).
- Un canal sécurisé par HTTPS pour échanger des informations entre les machines, en utilisant un serveur (https://sync.cresus.ch) pour la coordination et le stockage des écritures et du plan comptable.
- Un canal sécurisé par HTTPS pour l'envoi de notifications, ce qui permet d'annoncer à une machine que le mandat a été modifié et qu'une synchronisation est requise.

Stockage et transmission des informations

Les données des mandats (fichiers de comptabilité, facturation et salaires) sont stockées localement. Elles ne quittent jamais la machine et ne sont pas envoyées dans le cloud. Vos données vous appartiennent et nous n'avons aucun moyen technique d'y accéder.

Le mécanisme de synchronisation transfère des écritures comptables d'une machine à l'autre. Afin de pouvoir comptabiliser, les logiciels Crésus Facturation et Crésus Salaires ont besoin d'une copie du plan comptable (fichier `*.crp`). Celui-ci est transmis depuis la comptabilité vers les autres machines, à travers le cloud.

Le service chiffre toutes les données qui transitent par le canal HTTPS avec un algorithme AES (cryptographie à clé symétrique). La clé utilisée a une longueur de 256 bits et est générée de manière aléatoire (en utilisant des procédés cryptographiques reconnus). Nous ne faisons pas de lien entre la clé et l'identité et du mot de passe fournis par l'utilisateur.

La clé ne quitte la machine que lorsqu'elle est transmise volontairement au moyen du ticket que l'utilisateur peut générer à la demande (et stocker sur une clé USB, par exemple).

Le serveur (https://sync.cresus.ch) stocke exclusivement des données chiffrées. Il est hébergé en Suisse.

Risques et vecteurs d'attaque

Pour qu'un tiers puisse accéder aux écritures de la comptabilisation, au nom des fichiers du mandat ou au plan comptable, celui-ci doit (1) obtenir une copie des données cryptées et (2) disposer de la clé. Dans la mesure où la clé est stockée sur chaque machine synchronisée au sein d'un mandat, il appartient à l'utilisateur de garantir la confidentialité de celle-ci.

PA, 04.12.2016