Note :
Le chiffrement des données numériques durant la crise sanitaire

Table des matières

1 Avertissement

Cette note répond à **un besoin spécifique** posé dans la situation de crise sanitaire : celui de partager et transmettre des informations en utilisant des canaux non sécurisés : une pièce jointe transmise via une messagerie non sécurisée, un fichier de grande taille transféré au moyen d'une application de transfert de fichiers « grand public », etc. La protection des informations, particulièrement si elles comportent des données à caractère hautement personnel ou sensibles, s'avère indispensable. Le chiffrement des fichiers ou documents peut dans ces circonstances constituer un moyen pour assurer cette protection. Il s'agit là d'**une solution de dernier recours** qui ne saurait se substituer à une politique globale de la sécurité des flux d'information du Système d'Information reposant sur des solutions de type VPN, messagerie sécurisée, etc., politique qu'il sera indispensable de mettre en place dans l'après-crise.

2 Rappel

Lorsqu'elles circulent sur Internet (tout particulièrement via le courrier électronique) nos données peuvent être **très facilement** interceptées par un tiers. Pour éviter que la lecture de nos messages soit simple, il faut donc les **chiffrer**. De cette manière, vos messages ne transitent plus **en clair**.

Parce que les mots ont un sens nous allons distinguer le concept de **chiffrement** de celui de **cryptage** :

- le **chiffrement** c'est l'opération qui consiste à transformer un message à transmettre, dit « message clair », en un autre message, inintelligible pour un tiers, dit « message chiffré », en vue d'assurer le secret de sa transmission. **Chiffrer** c'est noter le message en un code conventionnel et secret. Seul celui qui possède le code (on parle de **clé**) sera en mesure de lire le message ;
- le terme **cryptage** n'a pas vraiment de sens en français (comme souvent en informatique c'est une mauvaise traduction de l'anglais). En revanche la cryptologie c'est l'étude des phénomènes cachés et par extension la science du chiffrement. **Décrypter** un message c'est l'opération qui consiste à tenter de lire un message dont on ne possède pas la clé.

3 Bref aperçu technique

Sommairement le chiffrage peut être effectué à 3 niveaux :

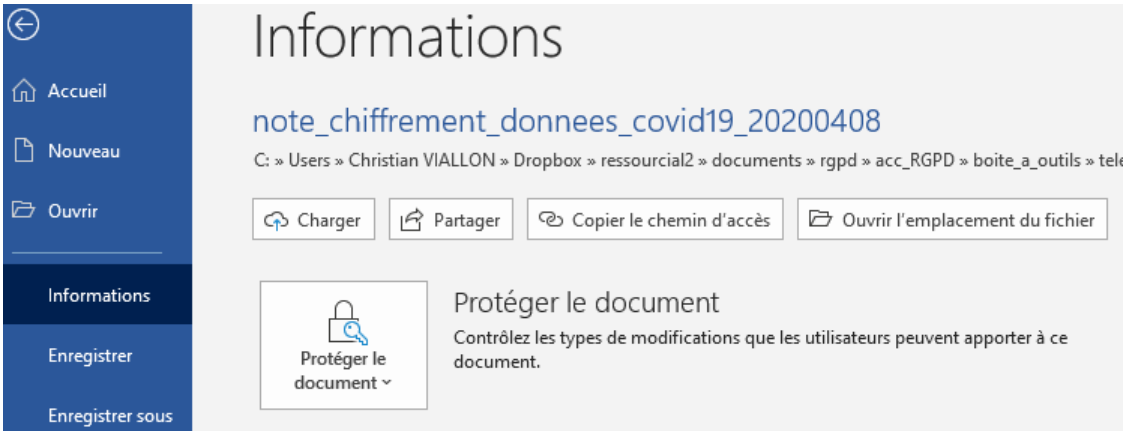
- le chiffrage du **canal de communication** : c'est le cas du VPN (Virtual Private Network pour réseau privé virtuel). Le VPN (pour être là encore très sommaire) consiste à annexer pour le seul usage de son organisation une partie de l'Internet ;
- le chiffrage du **protocole de communication** : c'est le cas par exemple du protocole https (HyperText Transfer Protocol Secure) qui consiste à combiner le protocole de l'hypertexte (http) avec une couche de chiffrement (SSL ou TLS) ;
- le chiffrage du **fichier** ou du document.

Dans cette note nous ne nous intéressons qu'au 3ème cas : le chiffrage du fichier ou du document.

4 Le chiffrage du fichier ou du document

Au moins **deux solutions** sont possibles :

- la première, très simple, consiste à protéger le document (Word ou Excel par exemple) par un mot de passe.
  Pour Word par exemple Fichier -> Informations -> Protéger le document



  Pour être simple, cette solution, est loin d'être infaillible (les logiciels de « crackage » circulent sur Internet). Elle est l'alternative minimum minimorum à la circulation en clair.

- la deuxième, un peu plus complexe, suppose d'utiliser un logiciel dédié.

5 Les logiciels open source dédiés au chiffrage

Certains logiciels permettent de chiffrer tout le disque dur ou la totalité d'un périphérique de stockage (clé USB, disque amovible, etc.), d'autres permettent de chiffrer des fichiers. Nous présentons ci-après une brève sélection de quelques outils de chiffrage. Il s'agit d'indications résultant de notre veille, elles ne dispensent pas d'évaluer les solutions proposées dont l'emploi se fait sous la seule responsabilité de l'utilisateur.

5.1 Chiffrer des fichiers

- AES Crypt (open source) : https://www.aescrypt.com/
- 7Zip (open source) : https://www.7-zip.org/
- AxCrypt (freemium) : https://www.axcrypt.net/fr/

5.2 Chiffrer tout le disque dur

- BitLocker : https://www.microsoft.com/fr-FR/download/details.aspx?id=7806
- VeraCrypt (open source) : https://www.veracrypt.fr/en/Home.html
- DiskCryptor (open source) : https://sourceforge.net/projects/diskcryptor/

5.3 Avantages et inconvénients des logiciels de chiffrage

- **le +** : le chiffrement est très robuste ;
- **le -** : le temps de prise en mains par l'utilisateur ;
- **le point de vigilance** : un fichier chiffré ne peut être ouvert que par l'utilisateur qui possède la clé ou le mot de passe. En l'absence de ces éléments (ou en l'absence/départ de l'utilisateur, perte de la clé ou du mot de passe) le fichier ne pourra être ouvert … et le chiffrement est, rappelons-le, très robuste !

6 Mode opératoire pour la transmission : deux canaux

L'opération de chiffrement génère un fichier codé qui ne peut être lisible qu'après déchiffrement. Le déchiffrement est rendu possible par l'utilisation d'**une clé** générée lors de l'opération de chiffrement. S'agissant de l'envoi d'un fichier chiffré à un correspondant, par exemple en pièce jointe à un mail, il est important de **séparer l'envoi du fichier chiffré de l'envoi de la clé**. Si le fichier chiffré est envoyé par courriel la clé est envoyée par SMS par exemple (ce serait la même opération pour un fichier Word ou Excel protégé par mot de passe).

7 Pour aller plus loin

Cette note est sommaire. Elle est destinée à apporter une aide dans l'urgence. Nous n'avons pas abordé les questions des VPN, de la messagerie sécurisée (notamment MSS messagerie sécurisée de santé), des coffres-forts numériques, etc. De même nous n'avons pas non plus traité des méthodes de chiffrement (symétriques, asymétriques).

Enfin nous sommes preneurs de toute contribution ou retour d'expérience permettant d'enrichir cette note.

8 Ressources CNIL :

- Chiffrer, garantir l'intégrité, signer : https://www.cnil.fr/fr/securite-chiffrer-garantir-lintegrite-ou-signer
- Les grands principes de la cryptologie et du chiffrement : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement
- Les ressources certifiées par l'ANSSI : https://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/#category_4