

Paris, le 16 janvier 2011



Direction générale
délégée aux ressources
www.cnrs.fr

3, rue Michel-Ange
75016 PARIS

Dossier suivi par Jean-Marc VOLTINI
jean-marc.voltini@dsi.cnrs.fr

Note à l'attention

des Directeurs d'Unité

Réf.Not11Y159DSI

Objet : Protection des ordinateurs portables

Les statistiques montrent que de nombreux ordinateurs portables sont régulièrement volés ou perdus au CNRS, nous exposant ainsi à la divulgation d'informations sensibles.

Lorsqu'il s'agit d'informations à forte valeur économique comme les documents préparatoires au dépôt d'un brevet ou que la loi oblige à protéger comme les données à caractère personnel, les conséquences juridiques, financières ou en termes d'image peuvent être particulièrement graves.

Une analyse des risques a montré que, peu ou prou, la plupart des ordinateurs portables sont susceptibles de contenir des informations sensibles, ne serait-ce que les codes permettant de se connecter au réseau ou d'accéder aux applications.

1 - L'orientation choisie : le chiffrement des ordinateurs portables

Le chiffrement étant une mesure efficace pour limiter les conséquences d'un vol ou d'une perte, il convient donc de chiffrer systématiquement tous les ordinateurs portables du CNRS. Cette orientation est en accord avec la demande du ministère de la Recherche.

Le CNRS a conduit une étude pour déterminer la solution la mieux adaptée à la diversité et l'envergure de son environnement informatique. Le choix a été fait d'une solution simple, présentant le minimum de contraintes pour les utilisateurs (généralement, il n'y a même pas à entrer un mot de passe supplémentaire).

2 - Le dispositif

Il repose sur une mise en œuvre à deux niveaux :

a) 1er niveau = protection de base, applicable à tous les ordinateurs portables

- Pour les nouveaux portables sous Windows et Linux : recours systématique aux disques chiffrants disponibles au marché DELL¹ (surcoût d'environ 30 €)
- Pour les portables anciens sous Windows : chiffrement du poste avec le logiciel TrueCrypt (qualifié par l'ANSSI, gratuit)
- Pour les portables anciens sous Linux : solutions natives de chiffrement des disques (dm-crypt)
- Pour les portables neufs et anciens Mac : solutions natives de chiffrement des disques (FileVault)
- Pour les clés USB : utilisation de clés USB auto-chiffrantes (pratiques d'utilisation et indépendantes des plates-formes utilisées), d'un modèle du commerce (payant), de préférence validé par le CNRS², ou à défaut utilisation de conteneurs TrueCrypt.

b) 2ème niveau = protection des données très sensibles

- Rajout d'une deuxième couche de chiffrement à la protection de base : les fichiers particulièrement sensibles sont, de plus, stockés dans des conteneurs chiffrés avec le logiciel TrueCrypt (qualifié par l'ANSSI³, certification CSPN⁴).

Le dispositif décrit ci-dessus n'est pas prévu pour la protection des informations classifiées de défense qui doit répondre à des règles propres⁵.

La protection des postes fixes, des serveurs et des échanges par messagerie seront traitées ultérieurement.

3 - Mise en œuvre et recouvrements :

Le chiffrement induit le risque de ne plus pouvoir accéder aux informations en cas d'oubli du mot de passe ou d'absence de son détenteur. C'est pourquoi il est nécessaire de mettre en place un mécanisme de recouvrement pour récupérer, le cas échéant, les codes d'accès. Cela s'effectue par le séquestre des mots de passe et des métadonnées associées dans un coffre-fort physique ou électronique.

Un guide d'installation sera prochainement envoyé au réseau des CSSI (Chargés de Sécurité des Systèmes d'Information), ASR (Administrateur Systèmes et Réseaux des Unités) et RSI (Responsable des Systèmes d'Information) des Délégations. Le RSI jouera le rôle de correspondant dans le cas où il n'y aura pas d'informaticien local.

Vous pouvez d'ores et déjà commander vos PC avec l'option « disque chiffrant » (via le marché Dell du CNRS).

¹ Disques Seagate certifiés FIPS 140-2 et SSD Samsung en cours de certification FIPS 140-2

² Marque CORSAIR, disponible sur Internet (d'autres modèles pourront être communiqués par la suite)

³ ANSSI - Agence Nationale de Sécurité des Systèmes d'Information

⁴ CSPN - Certification de Sécurité de Premier Niveau

⁵ A définir avec le Fonctionnaire de Sécurité Défense

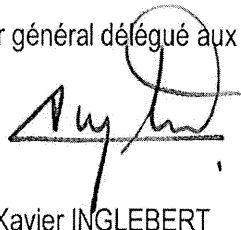
4 - Avertissement

Cette nouvelle mesure de protection ne dispense pas de vigilance contre le vol, de sauvegarde régulière des données ainsi que des autres mesures classiques de protection.

Par ailleurs, certains pays restreignent ou interdisent l'usage du chiffrement⁶. Les voyageurs qui s'y rendent doivent alors utiliser une machine dédiée à cet usage, contenant le minimum d'informations, qui sera réinstallée avant le départ et après le retour comme cela est indiqué dans le *Passeport de conseils aux voyageurs*⁷.

Il est de la responsabilité du directeur d'unité de s'assurer que des mesures de protection des données sont bien mises en œuvre.

Le Directeur général délégué aux ressources



Xavier INGLEBERT

⁶ http://www.securite-informatique.gouv.fr/gp_article714.html

⁷ http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

ANNEXE

Choix d'une solution de chiffrement

Le but de ce document est de présenter la démarche ayant conduit à la recommandation sur le chiffrement.

Analyse des risques

Si la facilité de transport d'un ordinateur portable est un atout indéniable pour le confort et la productivité de son utilisateur, c'est aussi une vulnérabilité car le vol ou la perte en est d'autant plus aisé.

Au-delà de la perte directe que cela représente : achat d'une nouvelle machine, temps perdu, coût de restauration des données, il faut évaluer les conséquences, à plus ou moins long terme, liées à la divulgation d'informations sensibles. On peut en citer quelques-unes :

- Juridiques lorsque la loi ou un contrat impose de protéger ces informations ;
- économiques avec l'impossibilité de déposer un brevet ;
- dégradation de l'image ou de la réputation ;
- perte de crédibilité interdisant de participer à de nouveaux projets ;
- atteinte à la sécurité du chercheur ou de ses contacts si certaines informations tombent en de mauvaises mains

Les statistiques montrent que les vols ou les pertes sont relativement fréquents. S'il faut effectuer une distinction entre les motivations des voleurs, opportunistes qui recherchent un matériel pour le revendre ou bien personnes malveillantes ciblant spécifiquement des informations, il reste que la menace est forte.

La conjugaison d'une forte menace, d'une grande vulnérabilité et de graves conséquences, fait que le risque doit être considéré comme élevé et, de fait, inacceptable en l'état. Le seul élément sur lequel on puisse réellement agir est la limitation des conséquences. La mise en place d'une mesure de chiffrement va permettre d'empêcher un éventuel voleur de récupérer les informations sensibles.

Il existe deux classes de produits de chiffrement dont nous allons détailler les caractéristiques :

- chiffrement de fichiers ;
- chiffrement du disque.

Chiffrement de fichier

- Le contenu du fichier ou de l'ensemble des fichiers d'un répertoire est chiffré.
- **Le nom et les métadonnées décrivant le fichier ne sont pas chiffrés. Le nom d'un fichier qui est souvent très explicite, est en lui-même une information sensible.**

• Bien des informations potentiellement sensibles peuvent se trouver ailleurs sur le disque sans que le propriétaire en ait nécessairement conscience :

- fichier d'échange (swap),
 - fichier d'hibernation (mise en veille prolongée),
 - fichiers temporaires,
 - cache Internet,
 - base de registre.
- Sauvegarde possible des fichiers sans avoir à les déchiffrer.
 - Tant que l'on n'a pas fourni le mot de passe pour déverrouiller un fichier ou un répertoire son contenu en clair est inaccessible.
 - Possibilité de confier la machine à un administrateur pour des opérations de maintenance sans qu'il puisse accéder aux fichiers chiffrés.
 - Possibilité de définir des listes de personnes de confiance qui auront accès aux fichiers chiffrés.
 - **L'utilisateur doit décider ou non du chiffrement du fichier.**
 - Historiquement ce sont les premières solutions qui sont apparues.
 - Exemples de solutions :
 - EFS (Windows)
 - ZoneCentral (Windows)
 - eCryptfs (Linux)
 - PGP et ses dérivés comme GnuPG
 - McAfee Endpoint Encryption for File/Folder

Chiffrement du disque

- Le contenu intégral du disque, d'une partition ou d'un volume logique (conteneur) est chiffré.
- **Aucune information n'échappe au chiffrement.**
- **Tranquillité d'esprit pour l'utilisateur qui sait que tout est chiffré.**
- Les sauvegardes ne peuvent s'effectuer qu'après déchiffrement ou alors il faut sauvegarder le disque ou volume entier (sauvegardes incrémentales impossibles).
- **Dès le démarrage, après fourniture du mot de passe tout le contenu du disque est accessible en clair.**
 - La personne en charge de la maintenance du système a accès à l'ensemble des informations du disque.
 - Transparence totale pour l'utilisateur.
 - Exemples de solutions :
 - Disques chiffrants (matériel)
 - BitLocker (Windows)
 - Dm-crypt (Linux)
 - FileVault (Mac OS)
 - TrueCrypt (Windows, Linux, Mac)

- PGP Whole Disk Encryption (Windows, Mac OS)
- McAfee Endpoint Encryption for PC (Windows)
- Check Point Full Disk Encryption (Windows, Mac OS, Linux)

Critères de choix

- Il s'agit de se protéger contre les conséquences du vol ou la perte d'une machine arrêtée. Le chiffrement ne permet pas de se prémunir contre la divulgation d'informations à la suite du vol d'une machine allumée.
- La solution ne s'adresse pas à des informations classifiées de défense.
- **L'usage doit être le plus simple et transparent possible pour l'utilisateur.**
- **Le déploiement doit poser le minimum de contraintes à l'administrateur.**
- Il faut se prémunir contre le fait que l'utilisateur, par mégarde, stocke des informations sensibles non chiffrées.
- Le produit de chiffrement doit être sûr au niveau cryptographique et si possible qualifié ou certifié.
- La solution doit être acceptée par les utilisateurs.
- Le coût doit être raisonnable.
- L'utilisation de dispositifs matériels de sécurité comme des cartes à puces ou des tokens est exclue car trop lourde et coûteuse à mettre en œuvre.
- **La solution doit s'adapter à la très grande diversité des environnements dans les différentes unités du CNRS.**
 - La solution doit faciliter le recyclage ou la mise au rebut du matériel.
 - **Une solution simple applicable systématiquement à toutes les machines ce qui n'exclut pas une solution optionnelle pour protéger quelques fichiers particulièrement sensibles.**

Analyse des différentes solutions

Seul le chiffrement intégral du disque permet de garantir que toutes les informations sensibles seront systématiquement chiffrées.

Si avec les processeurs modernes la charge supplémentaire introduite par le chiffrement est le plus souvent faible, il ne faut pas négliger le facteur psychologique qui attribuera, généralement à tort, tout ralentissement de la machine au chiffrement.

Le recouvrement aussi indispensable soit-il n'est pas un facteur discriminant. En effet la méthode est toujours la même, il s'agit du séquestre d'un mot de passe. Le rangement d'une copie dans une enveloppe stockée dans une armoire sécurisée ou un coffre-fort est parfaitement satisfaisant. Les demandes de recouvrement devraient rester rares, en effet, surtout avec un mécanisme de mot de passe unique, il y a assez peu de chances qu'un utilisateur oublie son mot de passe principal.

Il existe de nombreux fournisseurs de produits de chiffrement. Tous les grands acteurs de la sécurité ont mis à leur catalogue, souvent à la suite de rachats, des produits de chiffrement. La

cohérence avec les autres outils de sécurité de la gamme (antivirus, etc.), une console d'administration unique est un atout. Dans le contexte du CNRS où il n'y a ni homogénéité du parc, ni administration centralisée l'argument a moins de valeur.

Disque chiffrant

- Chiffrement matériel au niveau du disque
 - Le chiffrement est toujours activé
 - Fonctionne sous Windows et Linux
 - Existe à la fois pour les disques classiques et les SSD
 - Disponibles dans le cadre du marché sur les portables Dell
 - Certification FIPS-140-2 pour les disques vendus par Dell
 - **L'authentification se fait au démarrage (pré-boot) à l'aide d'un mot de passe. Il n'est pas nécessaire de fournir à nouveau un mot de passe pour ouvrir une session Windows.**
 - **Aucune perte de performances liée au chiffrement**
 - Aucune clé de chiffrement ne réside en mémoire de l'ordinateur ce qui prémunit contre les attaques cherchant à récupérer des clés en mémoire (« cold boot attack⁸ » par exemple)
 - Sans connaissance du mot de passe, il est impossible de modifier le code de démarrage ce qui rend impossible les attaques du type « evil maid⁹ »
 - Sans connaissance du mot de passe un disque ne peut être utilisé, pas même réinitialisé ce qui en ôte toute valeur pour un éventuel voleur
 - Surcoût modéré (~30€)
 - Recouvrement : séquestre du mot de passe administrateur du disque
 - Le disque est chiffré en permanence ce qui dispense du chiffrement initial du disque qui peut prendre plusieurs heures avec les solutions logicielles
 - Une commande permet de réinitialiser, en quelques secondes, le disque avec attribution d'une nouvelle clé symétrique de chiffrement ce qui facilite le recyclage ou la mise au rebut
- Du fait de ses performances, de sa sécurité, de sa totale transparence c'est la solution de choix.**

TrueCrypt

- Logiciel disponible sous Windows, Linux et Mac
- Chiffrement d'un conteneur (volume logique)
- Les conteneurs chiffrés peuvent être accédés indifféremment sous Windows, Linux et Mac.
- Chiffrement intégral du disque avec authentification au démarrage (pré-boot) uniquement pour Windows
- Qualifié et certifié premier niveau par l'ANSSI

⁸ http://en.wikipedia.org/wiki/Cold_boot_attack

⁹ http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Veilletechnologique/evil_maid_attack/

- Logiciel ouvert et gratuit

- Recouvrement : sauvegarde des métadonnées et du mot de passe utilisé lors de la création

Sous Windows c'est un logiciel de chiffrement intégral de disque qui a l'avantage d'être gratuit et certifié. Pour l'échange entre machines de conteneurs, c'est le seul qui soit multiplateforme (Windows, Linux, Mac)

FileVault

- **Inclus dans le système Mac OS X**
- Le répertoire de l'utilisateur est chiffré (dans un volume logique chiffré)
- Le système n'est pas chiffré
- Il est possible de chiffrer le fichier d'échange (swap) et le fichier d'hibernation (mise en veille prolongé)
- **La mise en œuvre est très simple, quelques cases à cocher**
- **Utilisation transparente, un seul mot de passe à saisir**
- Recouvrement : séquestre d'un mot de passe administrateur

Il n'y a guère d'autres solutions pour les ordinateurs Mac.

Dm-crypt

- **Inclus dans la plupart des distributions Linux (la procédure d'installation demande si on veut ou non utiliser le chiffrement)**
- Chiffrement d'une partition, une petite partition servant au démarrage (boot) reste non chiffrée mais elle ne contient rien de sensible
- **Logiciel ouvert et gratuit**
- Un mot de passe est à fournir lors du processus de démarrage
- Recouvrement : séquestre d'un mot de passe

Lorsqu'il n'est pas possible d'utiliser des disques chiffrant, c'est la solution pour Linux.

ZoneCentral

- Uniquement pour Windows, certifié par l'ANSSI, payant
- Chiffrement de tous les fichiers d'un ou plusieurs répertoires et sous répertoires
- Choix de l'authentification : certificat ou mot de passe
- **Un certain nombre de fichiers du système dont le fichier d'hibernation ne peuvent être chiffrés**
- **Nombreux paramétrages possibles ce qui offre une grande souplesse mais complique singulièrement le déploiement, l'utilisation d'Active Directory et de GPO est recommandé**
- Recouvrement : séquestre du mot de passe ou d'un certificat d'un agent de recouvrement
- Utilisé au CNRS dans le cadre d'une opération pilote

Ce produit ne peut chiffrer que partiellement le disque, aussi il ne peut être recommandé comme solution de base (1er niveau - cf. chapitre suivant « Recommandations »).

Recommandations

Le dispositif repose sur des solutions à deux niveaux :

1er niveau = protection de base, devant être appliquée à tous les ordinateurs portables :

- Pour les nouveaux portables sous Windows et Linux : recours systématique aux disques chiffrants disponibles au marché DELL¹⁰
- Pour les portables anciens sous Windows : chiffrement du poste avec le logiciel TrueCrypt (qualifié par l'ANSSI)
- Pour les portables anciens sous Linux : solutions natives de chiffrement des disques (dm-crypt)
- Pour les portables neufs et anciens Mac : solutions natives de chiffrement des disques (FileVault)
- Pour les portables actuellement chiffrés avec ZoneCentral : possibilité de conserver la solution selon contexte
- Pour les clés USB : utilisations de clés USB auto-chiffrantes d'un modèle du commerce, validé de préférence par le CNRS¹¹ (pratiques d'utilisation et indépendantes des plates-formes utilisées), ou à défaut utilisation de conteneurs TrueCrypt.

2ème niveau = protection des données très sensibles :

Rajout d'une deuxième couche de chiffrement à la protection de base : les fichiers particulièrement sensibles sont stockés dans des conteneurs chiffrés avec le logiciel TrueCrypt (qualifié par l'ANSSI, certification CSPN).

¹⁰ - Disques Seagate certifiés FIPS 140-2 et SSD Samsung en cours de certification FIPS 140-2

¹¹ - Marque CORSAIR, disponible sur Internet.