Questions fréquentes relatives à la note « chiffrement » réactualisée

Version	Date	Rédaction
1.0	06/12/2018	Michel CHABANNE, RSSI CNRS

Table des matières

Portée de l'obligation de chiffrement

Tous les ordinateurs professionnels de l'unité, quelle que soit la source de financement, sont soumis à l'obligation de chiffrement intégral des disques. Cette règle souffre des exceptions, qui sont uniquement motivées par :

- l'absence de stockage de données de recherche, de données sensibles au sens de la PSSI, l'absence de données à caractère personnel de tierces personnes ;
- l'incapacité technique à chiffrer (indisponibilité de la fonction logicielle, obsolescence non résorbable pour des raisons techniques ou de coût, trop faible puissance du système…) ;
- l'impossibilité de mettre en œuvre le chiffrement à cause d'un impact réel et démontrable sur le fonctionnement du système, l'empêchant réellement d'accomplir ses tâches (système temps réel…) ;
- la fugacité des données à protéger (cluster de calcul) ;
- les conditions matérielles d'hébergement rendant trop peu probable un vol de l'équipement. Dans beaucoup de cas, les espaces de travail habituels sont encore trop peu sécurisés pour rendre le vol improbable.

Un système d'exploitation obsolète sur une machine de moins de 5 ans n'est pas un motif d'exception. Sauf obligation impérieuse liée par exemple à l'exécution d'un logiciel très particulier, le système doit être mis à jour et le chiffrement activé, conformément à la PSSI.

Si le directeur d'unité autorise, dans la PSSI du laboratoire, l'utilisation d'ordinateurs **personnels** à des fins professionnelles, des mesures de protection des données professionnelles doivent être mises en place. Il s'agit par exemple de conteneurs chiffrés à l'aide d'un logiciel comme Veracrypt. Pour rappel, dans une unité ZRR, l'usage d'ordinateurs personnels ne doit pas être autorisé.

Concernant les smartphones, ceux qui sont fournis dans le cadre professionnel sont chiffrés avant leur mise à disposition des utilisateurs. Un code de verrouillage est appliqué, 8 caractères étant une longueur nécessaire au vu de l'entropie résultante. Il faut noter que la plupart des smartphones modernes sont chiffrés par défaut lorsque le code de verrouillage est positionné (Android depuis 5.0 [2014] au premier démarrage, iOS depuis iPhone 4). La robustesse de ce chiffrement dépend directement de la force du code de verrouillage qui est utilisé. Il est nécessaire de chiffrer l'ensemble du smartphone, carte SD éventuelle incluse.

Concernant les serveurs, l'obligation de chiffrement ne porte que sur les équipements stockant des données de recherche ou des données à caractère personnel de tiers en nombre significatif. Les serveurs ancillaires (DHCP, DNS, NTP) ne sont pas concernés. La priorité doit s'apprécier encore selon la vraisemblance du risque de vol : ce risque dépend directement des mesures de contrôle d'accès physique à l'environnement du serveur. Si ce dernier est dans un simple bureau ou un local mal protégé, le risque est considéré comme important. Dans une salle serveur avec contrôle d'accès correctement géré, le risque est faible.

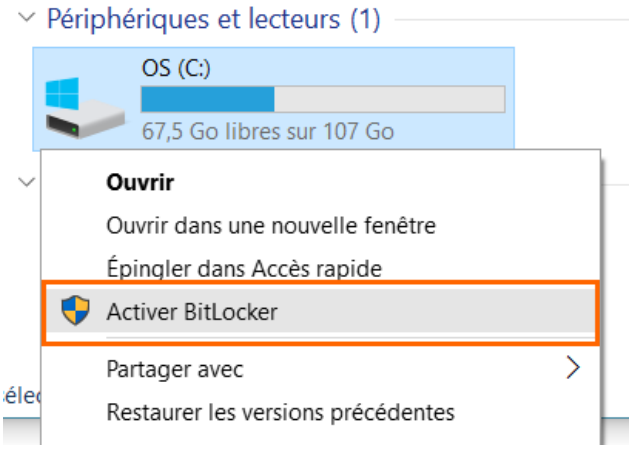
Le vol touche aussi bien les portables que les fixes. Les incidents récents montrent une hausse des intrusions physiques dans les unités avec vol de matériel à la clé. La protection des postes fixes ne doit donc pas être négligée.

Comment savoir si mon système est chiffré

Il est difficile d'être exhaustif, mais concernant les plateformes logicielles principales.

Windows 10

Si le menu « Activer Bitlocker » apparaît lors d'un clic droit dans l'explorateur sur le disque C:, le PC n'est **PAS** chiffré



Mac OS

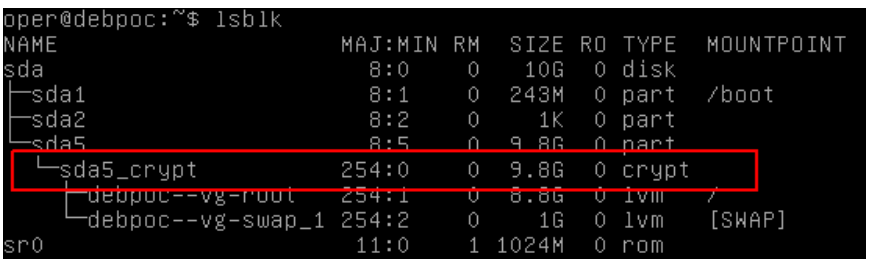
Sélectionnez Menu Apple > Préférences Système et cliquez sur Sécurité et confidentialité. Cliquez sur l'onglet FileVault.
La phrase « Filevault est activé » indique que le chiffrement est **actif**.

Linux

En ligne de commande :

```
# lsblk
```

Exemple de retour de la commande sur un système **chiffré**.



Android

Dans le menu « Paramètres » > « Sécurité », vérifiez le menu « Chiffrer le téléphone », qui doit mentionner « chiffré ». Si cette fonction est absente du terminal, il ne DOIT PAS être utilisé à des fins professionnelles.

iOS (IPhone)

Dans le menu « Paramètres » > « Touch ID et mots de passe » > en bas de l'écran s'affiche « la protection des données est active ».

Conseils pour Linux

Il est fortement conseillé, lors de la mise en œuvre du chiffrement :

- de sauvegarder les en-têtes (*LUKS header*) du disque dur
- de positionner une clé de recouvrement, qui peut être unique pour l'unité

Cette page[1] décrit les commandes standards pour réaliser ces actions.

Quelle priorité donner aux différents supports à chiffrer

Deux critères doivent gouverner la priorisation des actions :

- en fonction de la vraisemblance du risque de vol/perte
- en fonction de la sensibilité des données.

Globalement, on peut établir la liste de priorité suivante :

- Périphériques ultramobiles (stockage externe, smartphones, portables)
- Ordinateurs fixes
- Serveurs concernés par l'obligation

Modalités de déploiement et de contrôle sur un parc important

Il est primordial de mettre en œuvre une solution logicielle de connaissance et de gestion du parc informatique de l'unité. Cet outillage permet une vision globale de l'état de sécurité du parc (fixes et portables *a minima*). Pour le suivi du chiffrement avec GLPi/OCSInventory, un plugin a été développé pour vérifier l'état du chiffrement[2].

Pour les environnements à dominante Windows, l'utilisation des outils proposés par l'éditeur (Active Directory et les GPOs, MDOP[3] comprenant Microsoft Bitlocker Administration and Monitoring) est un facilitateur évident. Les clés de recouvrement peuvent être stockées dans Active Directory. La protection des contrôleurs AD nécessite bien sûr une vigilance particulière.

Responsabilités en cas de contrôle

Le Directeur d'Unité est responsable du déploiement de la consigne de chiffrement dans son unité. Le CSSI (chargé de SSI dans l'unité) et l'Administrateur Système ont la charge de l'assistance technique au déploiement.

Il n'est pas autorisé de faire signer quelque « décharge » ou « engagement » que ce soit à l'utilisateur qui refuserait le chiffrement.

En cas de refus, la situation doit être remontée et motivée à la Direction de l'Unité qui a la charge :

- de vérifier avec l'appui du CSSI/ASR que l'exemption du chiffrement est applicable
- de rappeler les enjeux, les objectifs et les risques encourus par l'utilisateur en cas d'absence de chiffrement.

Si le différend persiste, le Délégué Régional joue le rôle de médiateur et d'arbitre, avec l'appui du RSSI-DR.

---

[1] Voir par exemple https://www.lisenet.com/2013/luks-add-keys-backup-and-restore-volume-header/
[2] https://github.com/PluginsOCSInventory-NG/bitlockerstatus
[3] https://partner.microsoft.com/fr-fr/solutions/mdop

Les ordinateurs de l'unité sont gérés avec l'appui d'un service partenaire

L'obligation de chiffrement pour les données sensibles dérive de la mise en œuvre de la PSSI de l'Etat qui s'impose à tous les services centraux et déconcentrées de l'Etat, à tous les établissements publics.

Tout différend sur la mise en œuvre de la consigne par un partenaire doit être remonté à la Délégation Régionale qui prend attache avec le partenaire et s'assure de sa compréhension des enjeux.

Chiffrement des sauvegardes

Le chiffrement des sauvegardes est une pratique nécessaire lorsque l'évaluation des risques de perte ou de vol identifie un risque non nul.

La fonction de chiffrement à la source est disponible dans des produits libres comme backuppc, commerciaux comme Veeam Backup, Atempo TiNa. Le chiffrement de surface du stockage cible peut être considéré comme suffisant. Un chiffrement logiciel est également disponible et doit être activé sur des équipements de type NAS (TimeCapsule Apple, Synology…).

Quelle confiance dans le chiffrement à l'aide de logiciels non qualifiés (Bitlocker, Filevault…)

L'objectif de la consigne est de limiter les conséquences de la perte ou du vol des équipements. Il ne s'agit pas de limiter les risques d'intelligence économique. Pour cela, dans le cas des ZRR, l'utilisation de logiciels de chiffrements qualifiés (PrimX Cryhod[4], éventuellement Veracrypt) est obligatoire.

Usage du chiffrement à l'étranger

Lorsque l'utilisateur voyage à l'étranger dans des pays où le chiffrement est prohibé ou lorsque les services de police ont le droit de demander le déchiffrement de l'équipement à l'entrée, il est nécessaire d'utiliser pour la mission un ordinateur dédié à cet effet, blanchi et ne comportant que les données nécessaires à la mission.

Si les services locaux de police demandent le déchiffrement ou retiennent l'ordinateur, l'utilisateur prévient immédiatement le FSD du CNRS.

Quelles formations pour le chiffrement

Deux ANF ont été conduites ces trois dernières années sur le chiffrement. Des formateurs formés à cette occasion ont rejoué localement ces ANF dans de nombreuses régions.

Des documentations sont disponibles :

- Sur l'intranet du CNRS, rubrique « protection des données », menu « Décisions et notes »
- Sur l'extranet SSI pour les CSSI[5]

[4] Peut être acquis au travers des accords du Groupe Logiciels.

[5] https://extra.core-cloud.net/collaborations/RSSI-CNRS/SitePages/Accueil.aspx