

CHIFFREMENT DES PORTABLES UL

Pourquoi chiffrer ?

- ✓ **Les risques** : perte ou vol des ordinateurs portables

- ✓ **Protection des données** :
 - ✓ Données classifiées, personnelles
 - ✓ Obligations légales ou réglementaires
 - ✓ Patrimoine scientifique et technique
 - ✓ Données sensibles

- ✓ Un objectif de la **PSSI**

Problèmes

- ✓ Le chiffrement peut être traité d'un point de vue trop technique
- ✓ Responsabilité juridique vis à vis des données chiffrées
- ✓ Maintenance
- ✓ Assistance aux utilisateurs
- ✓ La sauvegarde des données doit continuer à être effectuée
- ✓ Gérer « l'indisponibilité » de l'utilisateur
- ✓ ...

Le Chiffrement

- ✓ **Le chiffrement n'est pas un problème technique**
- ✓ **Mais c'est avant tout un problème d'organisation et de mise en place de procédure**

Recouvrement, séquestre

- ✓ En cas de vol, panne, ou perte de mot passe que fait-on ?
- ✓ Il faut mettre en place une procédure de **recouvrement**
- ✓ Il faut organiser un **séquestre**, c'est à dire pouvoir conserver de façon sécurisée :
 - ✓ Mot de passe utilisateur ou administrateur
 - ✓ CD de récupération
 - ✓ Clés
 - ✓ ...
- ✓ **Il faut pouvoir récupérer les données**

Autres exigences

- ✓ Il faut continuer à faire des sauvegardes :
 - ✓ Atempo Live Navigator (UL)
 - ✓ Compte rendu des sauvegardes
- ✓ Qualité du mot de passe user
- ✓ Qualité du mot de passe administrateur

logiciels / matériels

- ✓ **Logiciels :**
 - ✓ Solution « constructeur »
 - ✓ Truecrypt / veracrypt
 - ✓ FileVault
 - ✓ dm-crypt

- ✓ **Matériels :**
 - ✓ Disque SED (disque chiffrant)

Le Chiffrement des portables UL

✓ **Windows**

- ✓ Solution : **bitlocker**
- ✓ Pas disponible pour windows 7 Pro
- ✓ Version minimale : windows 8
- ✓ Clé de recouvrement
- ✓ Qualité du mot de passe utilisateur
- ✓ Ne pas stocker la clé dans l'environnement Microsoft Onedrive
- ✓ A étudier : le stockage dans l'AD UL

Le Chiffrement des portables UL

- ✓ **MacOS**
 - ✓ Solution : Filevault
 - ✓ Chiffre des conteneurs : home de l'utilisateur et protège la mémoire virtuelle
 - ✓ Clé de secours
 - ✓ Lié à chaque utilisateur du Mac
 - ✓ Ne pas stocker la clé de secours chez Apple et ne pas utiliser le compte icloud
 - ✓ Qualité du mot de passe utilisateur

Le Chiffrement

- ✓ Chiffrement de conteneurs (Truecrypt / Veracrypt)
- ✓ Disque externe
- ✓ Disque pour Time Machine
- ✓ Clé USB
 - ✓ Facile d'utilisation avec un logiciel de chiffrement ?
 - ✓ Fiabilité d'une solution matérielle (empreintes digitales)
- ✓ Téléphones (voir note DAT-NT-010/ANSSI/SDE/NP)

Conclusion

- ✓ Situation actuelle :
 - ✓ Quelques portables de la présidence
 - ✓ Organisation non formalisée

- ✓ Pour le déploiement à une plus grande échelle
 - ✓ Mise en place de procédure (transmission des clés, mots de passe, stockage, ...)
 - ✓ Organisation avec les CSSI
 - ✓ Sans doute un travail à faire en 2017