



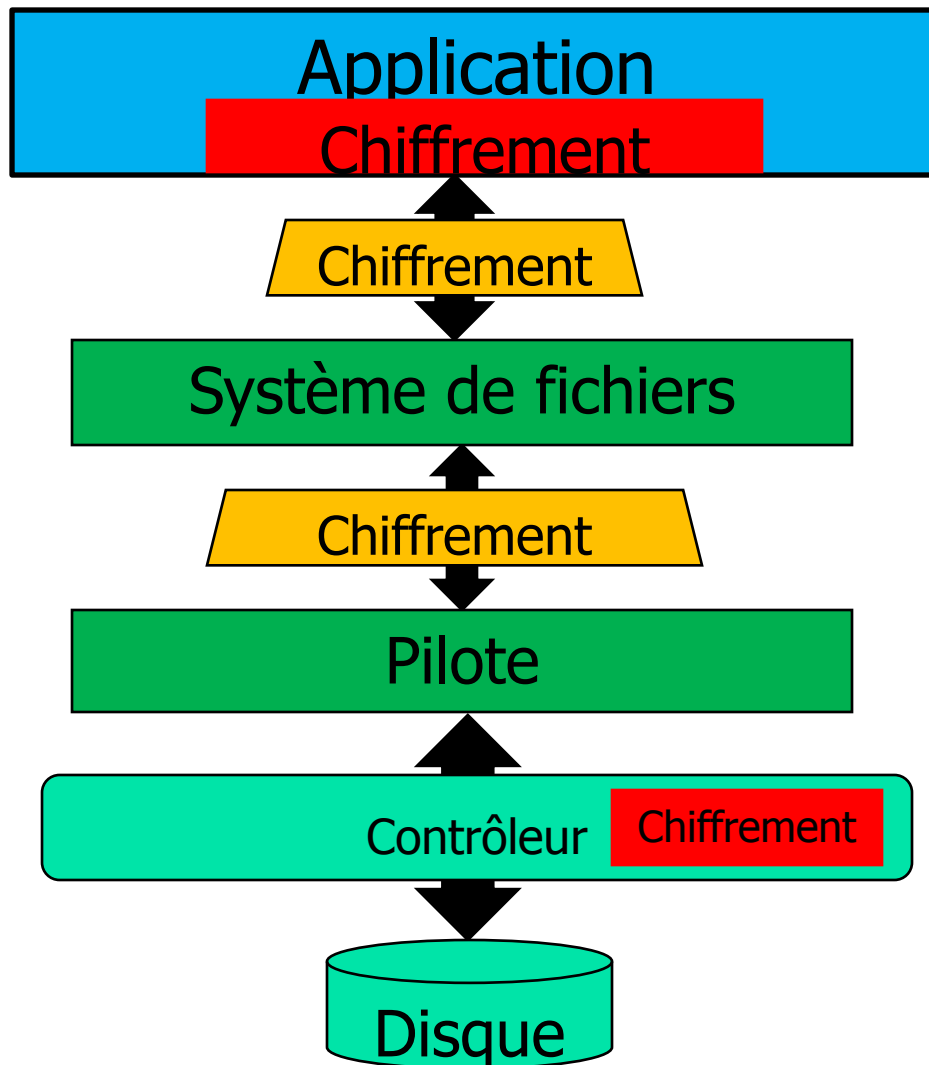
Besoins en matière de chiffrement et recommandations

Pourquoi chiffrer ?

- Protection contre les fuites d'information
 - Communications, échanges sur Internet
 - Ecoutes, interceptions
 - Perte, vol, emprunt temporaire
 - Ordinateurs portables
 - Supports amovibles
 - Serveurs, postes fixes : aspiration de données
 - Mise au rebut, réparation
- Assurer la confidentialité
 - Accès par les seules personnes autorisées : partages

- Utilisation des moyens de cryptologie : libre
 - LCEN art. 30
 - Longue histoire : de l'arme de guerre à la liberté
- Peines aggravées si utilisation du chiffrement dans la commission d'un crime ou délit
 - Code pénal 132-79
 - Sauf si fourniture des clés de déchiffrement
- Chiffrement interdit sans autorisation de l'employeur
 - Cour cassation 18/10/2006, Techni-soft
- Fourniture, importation, exportation de moyens de cryptologie : réglementée

Où chiffrer ?



Où trouver des données en clair ?

- Mémoire vive
- Fichiers temporaires
- Swap
- Dump en cas de crash du système
- Fichier d'hibernation (mise en veille)
- Informations dans les fichiers du système
 - Base de registres Windows
 - Secrets d'authentification (en particulier sous Windows)
 - Paramètres de connexion : noms de serveur, identifiants, etc.
 - Fichiers de configuration.
- Cache et historique du navigateur
- Métadonnées (nom de fichiers)

Quand trouver des données en clair ?

- La fenêtre d'exposition des données en clair varie en fonction de la méthode
 - Machine allumée : disque, partition
 - Du déverrouillage du répertoire ou fichier à sa fermeture : fichier, répertoire
- Maintien en cache des secrets servant au déchiffrement jusqu'à
 - Purge volontaire
 - Fermeture session

- Permettre au propriétaire ou à un tiers de récupérer les données si la clé n'est plus disponible
- Méthodes
 - Séquestre : duplicata de la clé ou du mot de passe en lieu sûr
 - Agent de recouvrement : un tiers a la possibilité de déchiffrer
 - Original disponible
- Organisationnel avant d'être technique
- Ne dispense pas des sauvegardes

- Protection physique
 - Sécurisation des locaux
 - Précautions lors du transport de données sensibles
- Communications
 - Protocoles sécurisés : SSL/TLS, IPSec, SSH, OpenVPN...
- Courrier électronique, échanges de documents
 - S/MIME
 - A défaut archive zip chiffrée

- Ordinateurs portables
 - Chiffrement intégrale du disque
 - Disque chiffré
 - Windows
 - Bitlocker
 - SafeBoot
 - EFS, ZoneCentral (pis aller)
 - Apple : File Vault
 - Linux : dm-crypt/cryptsetup (/home, /var, /tmp)

- Supports amovibles
 - Conteneur chiffré (disque virtuel)
 - Truecrypt
- Contrôle d'accès à des données partagées
 - Windows : ZoneCentral, EFS (1 seule machine)
 - MacOS : FileVault
 - Linux : Ecryptfs voire dm-crypt
- Chiffrement n'est pas une panacée
 - Poste de travail compromis
 - Autres canaux : imprimante, capture d'écran
 - Ingénierie sociale

- Simplicité
- Organisation du recouvrement, pour les différents produits
 - Une seule procédure de séquestre
 - Le même agent de recouvrement (certificat)
- IGC du CNRS
 - Ajout des attributs nécessaires aux différents produits de chiffrement
 - Certificats de chiffrement \neq authentification
 - Séquestre des certificats de chiffrement ?

- Couvrir l'ensemble des problématiques de chiffrement
- Objectifs déterminer
 - Ressources financières et humaines liées au déploiement
 - Besoins de formation et d'assistance
 - Acceptation par les utilisateurs
 - Vérification en situation réelle des procédures de recouvrement

- Résultat attendu, livrable
 - Liste de produits conseillés
 - Outils d'installation et déploiement (préconfiguré)
 - Documentation
 - Validation des procédures de recouvrement
 - Unification au niveau organisationnel malgré la diversité des produits
 - Mise en place d'assistance, de formation
 - Local (ASR) : hot line pour les utilisateurs
 - Régional (CRSSI) : conseil sur les choix à effectuer

- Appel à volontaires
 - Couvrir les différentes situations
 - Tester en situation réelle les produits
 - Préparer les kits d'installation
 - Rédiger la documentation