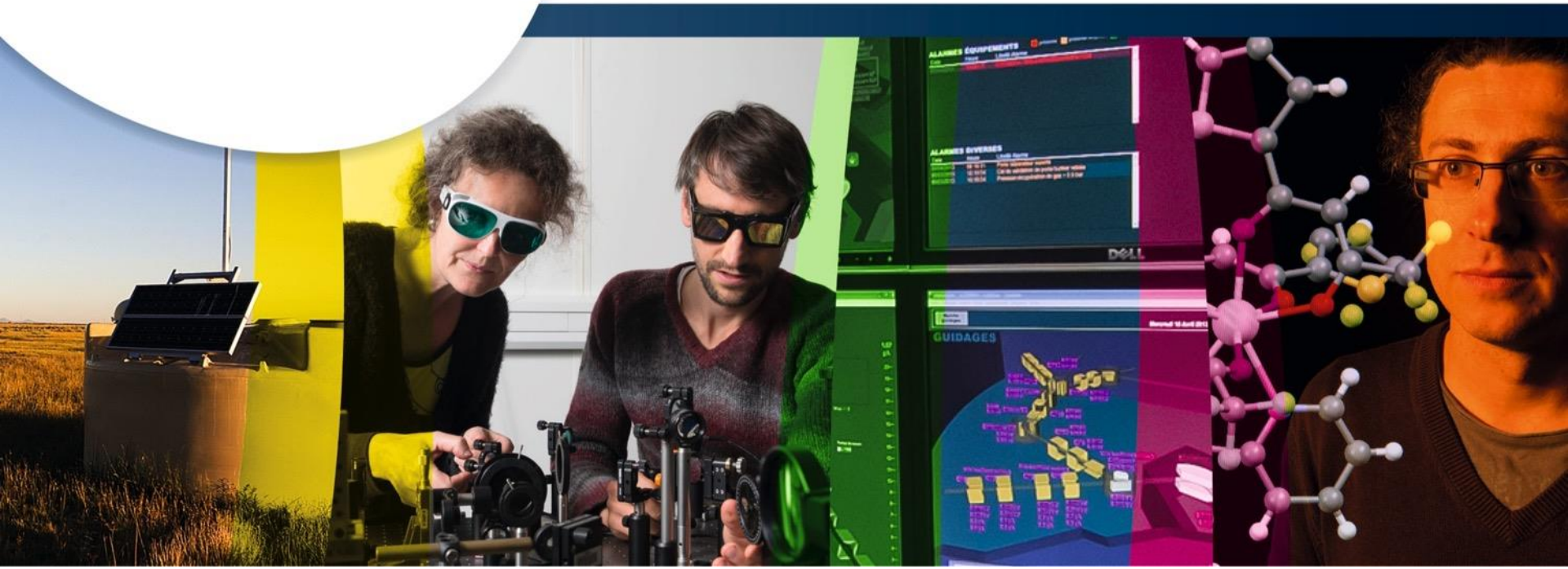
www.cnrs.fr

Chiffrement CNRS

2RCE Lorraine



Généralités

- Réglementation en France
  - Utilisation libre
  - Fourniture, importation, transfert intracommunautaire, exportation soumis sauf exception à déclaration ou autorisation
- Classement « double usage » (civil & militaire)
- Démarches auprès de l'ANSSI

Voir sur le site ANSSI :

http://www.ssi.gouv.fr/entreprise/reglementation/controle-reglementaire-sur-la-cryptographie/

Généralités

- Recommandations dans les annexes du RGS (Référentiel Général de Sécurité)
  confiance dans les échanges au sein de l'administration et avec les citoyens

– A1, A2, A3, A4, A5 : gestion des clés, IGC
– B1, B2 : mécanismes cryptographiques
– B3 : authentification

voir:
http://www.ssi.gouv.fr/entreprise/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/

PSSI - ETAT

- RES-PROT : protection des informations
  – […] Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté.

- EXP-PROT-INF : protection des informations sensibles en confidentialité et en intégrité
  – Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité.
  - A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

PSSI - ETAT

- EXP-MAINT-EXT : maintenance externe
  – Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique.
  Les opérations de chiffrement doivent faire appel à des produits qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.
- PDT-CHIFF-SENS : chiffrement des données sensibles
  – Une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

PSSI - ETAT

- PDT-NOMAD-STOCK : stockage local d'information sur les postes nomades

  - Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.

- • PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions

  – Les imprimantes et copieurs multifonctions hébergés localement dans une entité doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible.

PSSI - ETAT

- PDT-TEL-DECT : limiter l'utilisation du DECT
  – Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.

www.cnrs.fr

PSSI - CNRS

- PDI-2
  – Les documents électroniques doivent être stockés, manipulés, transmis via les procédures et avec les outils propres à assurer leur confidentialité au niveau adéquat.
- GRH-1
  – Le personnel entrant dans l'unité doit être accueilli suivant une procédure d'accueil formalisée qui inclut la prise de connaissance de la charte SSI et des règles élémentaires de sécurité informatique avant l'ouverture des accès sur le SI.
  • GRH-2
  – Le personnel en déplacement à l'étranger doit suivre une procédure formalisée permettant une gestion des matériels informatiques spécifique aux risques relatifs à ces déplacements.

Missions à l'étranger

- L'ANSSI
  - Guide Partir en mission
  - Passeport de conseils aux voyageurs
- Club des directeurs de sécurité des entreprises (CDSE) et le Centre de crise du ministère des Affaires étrangères
  - Passeport sur la sécurité des voyageurs salariés à l'étranger.
- Recommandations
  - Chiffrer lorsque c'est autorisé
  - Partir avec le minimum
  - Nettoyage avant et Nettoyage après
  - Transférer les informations via un canal chiffré lorsque c'est possible

www.cnrs.fr

Risques induits par le chiffrement

- Perte de disponibilité (perte d'informations)
  - Perte d'une passphrase, d'un certificat, ou d'un token par l'utilisateur
  - Altération ou perte des clés de chiffrement
  - Départ d'un utilisateur
  - Départ d'un administrateur système
  - Révocation ou expiration d'un certificat
  - Perte du matériel ou du logiciel ayant procédé au chiffrement
  - Altération ou perte du secteur d'amorçage du disque dur
  - Etc.

Risques induits par le chiffrement

- Perte de confidentialité (vol d'information)
  - Mot de passe faible
  - Coercition ou manipulation sur l'utilisateur, l'administrateur système (physique ou morale)
  - Cryptographie obsolète ou utilisation d'un algorithme de cryptographie « non-standard » et faible
  - Réinvention de l'implémentation de la cryptographie
  - Backdoor ou faiblesse dans les implémentations– KeyLogger et piégeage de matériel ou de logiciel
  - Réglementation (USA, Chine, Israël, etc.)
  - Séquestre non-sécurisé
  - Déchiffrement volontaire
  - Post-it
  - Etc.

Risques induits par le chiffrement

- Difficultés de fonctionnement
  - problématique de déploiement et de maintenance du chiffrement sur le parc
  - Problématique de maintenance des matériels chiffrés
  - Perte de performance des équipements pour l'utilisateur
  - Manque d'ergonomie des outils pour les administrateurs
  - La diversité des outils et les problématiques de compatibilité
  - Support à distance
  - Etc.

www.cnrs.fr

Mesures pour réduire ces risques

- Pour limiter la perte d'informations
  SAUVEGARDES « EN CLAIR » SECURISEES !
  – Gérées
  – Cloisonnées en fonction du niveau de sensibilité
  – Conservées dans un lieu physique sûr
  – Testées régulièrement

www.cnrs.fr

Mesures pour réduire ces risques

Séquestre :

Action de stocker de façon sécurisée les clés de chiffrement et ou les paraphrases pour pouvoir, le cas échéant, les restaurer.
SECURISER et SAUVEGARDER les séquestres

– Utilisation possible de KeePass
– Backup trueCrypt
– Mot de passe dans un fichier sur un autre support
– Etc.

Mesures pour réduire ces risques

- **Recouvrement** :

  Action de remettre au « clair » une information chiffrée suite à la perte d'une clé de chiffrement ou une passphrase.

  ● Le recouvrement, généralement effectué par un agent de recouvrement (le CSSI de l'unité?), consiste à rendre à l'utilisateur l'objet séquestré ou utiliser une clé ou une passphrase de recouvrement globale.

  ● SECURISER et SAUVEGARDER les dispositifs de recouvrement

  – Mot de passe de recouvrement (dmcrypt-luks)
  – Liste d'accès ZoneCentral
  – Mot de passe maître de FileVault2
  – Etc.

Mesures pour réduire ces risques

- Pour limiter le vol d'information : **Sensibiliser l'utilisateur**

– Taille des mots de passe
– Le danger des post-it
⇒ les accompagner vers les certificats quand c'est possible
– La nécessite du chiffrement
⇒ Protection du potentiel scientifique et technique
⇒ Conserver les capacités de valoriser les résultats de la Recherche
– Les missions à l'étranger : Partir avec des terminaux « blanchis

www.cnrs.fr

Quelques références CNRS

- Le site collaboratif du RSSI du CNRS
  https://extra.core-cloud.net/collaborations/RSSI-CNRS
  – Documentation sur les produits recommandés par le CNRS
  – Divers procédures liés à ces outils
  – Hygiène informatique de base pour les terminaux et les serveurs
  – Déclaration des incidents (vol, etc.)
  – Enquête « chiffrement »

- La liste « chiffrement »
  https://listes.services.cnrs.fr/wws/info/chiffrement

Chiffrement - CNRS

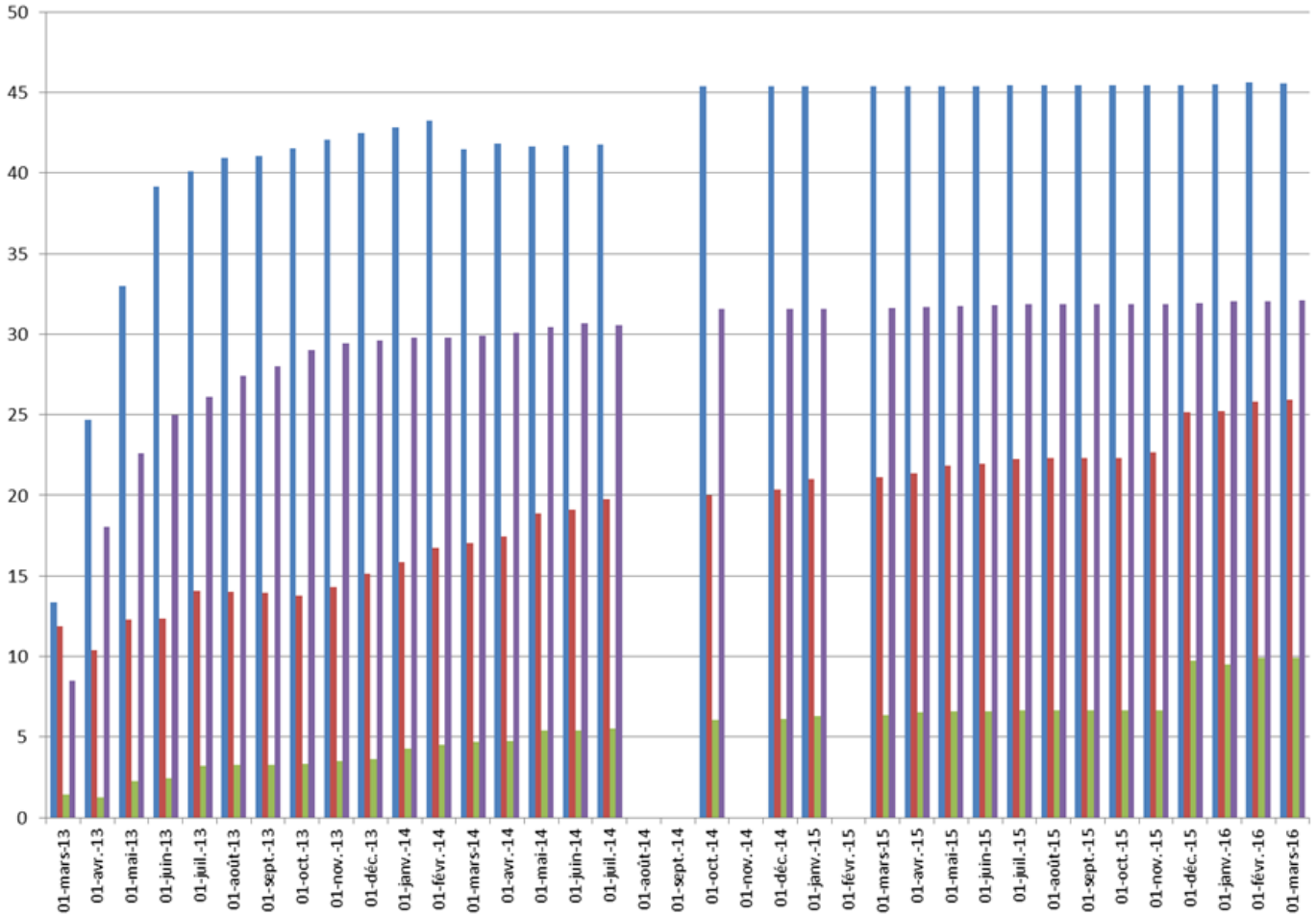
- Note du Président aux DU sur le vol d'ordinateurs (21 décembre 2012)
  - Note du DGD-R aux DR sur le vol d'ordinateurs (21 décembre 2012)

www.cnrs.fr

- En clair, il faut chiffrer les ordinateurs

Tableau de bord CNRS sur le chiffrement

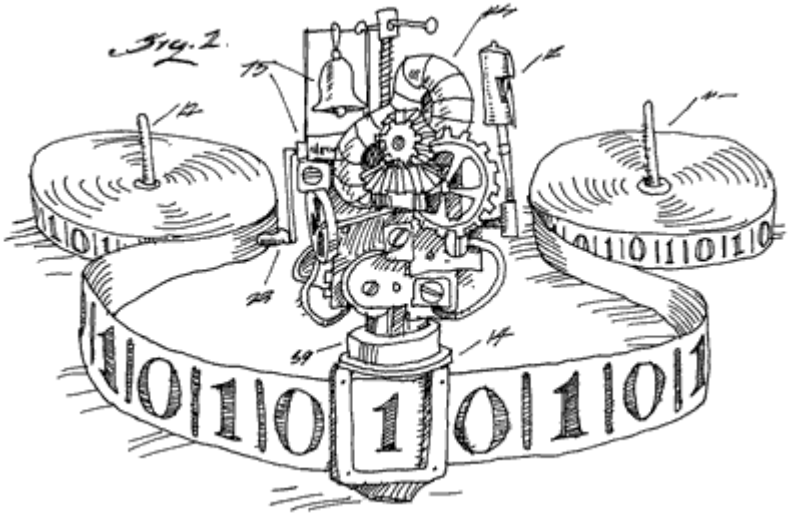
www.cnrs.fr



- % unités qui déclarent le suivi
- % de portables chiffrés
- % de fixes chiffrés
- Nb de portables déclarés en milliers

Questions ?

www.cnrs.fr



- Merci à Jérémie Boutard et François Morris (DSI – CNRS)