



CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Protection et chiffrement de données sensibles

Présentation des opérations pilotes de chiffrement





Distinction « classifié » et « sensible »

Les données « classifiées » : (instruction 900)

- Très Secret Défense
- Secret Défense
- Confidentiel Défense

⇒ Accès à ces données subordonnée à une « habilitation » des personnes au niveau équivalent

• Les données « sensibles » : (instruction 901)

données dont la **divulgation** ou l'**altération** ou la **non-disponibilité** porterait un préjudice aux intérêts fondamentaux de la nation ou à des tiers (personnes morales et personnes physiques) : données scientifiques, techniques, privées

Mentions utilisées « confidentiel ... », « diffusion restreinte » etc...



Typologie des données sensibles

Données de gestion interne

- Données à caractère nominatif
- Certaines données comptables ou financières
- Données à caractère politique ou stratégique

Données du patrimoine scientifique et technique

- Données relatives à des compétences ou des savoir faire internes
- Données relatives à la valorisation des résultats de la recherche
- Données relatives aux coopérations nationales et internationales
- Données scientifiques et techniques (travaux et résultats de recherches ayant un caractère appliqué ou lié à des savoir faire), /défense ou technologies de pointe
- Données scientifiques et techniques dont la confidentialité est imposée dans le cadre de contrats industriels (données “ confidentiel industriel ”)

Liste de « technologies sensibles » arrêtées par le SGDN (liste confidentiel défense)

Données diverses de sécurité

Données à caractère non scientifique touchant à des incidents internes, à la prévention, aux classements de sensibilité, aux plans de protection etc...)



L'impératif de protection des données sensibles

La non protection des données classifiées (=> risques de compromission de données)

= code pénal (articles 413-9 à 413-12)

La non protection des données sensibles non classifiées

- Atteintes au patrimoine scientifique (dommages pour la nation, l'établissement, le laboratoire, ...)
- Atteintes aux personnes (peuvent aussi relever du **code pénal** : cf. **article 226-17** « *sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations ...* »)



Protéger

QUOI ?

POURQUOI ?

COMMENT ?



QUOI ? POURQUOI?

- Identifier les données sensibles
- Evaluer leur niveau de sensibilité
- Identifier les menaces, leur probabilité
- Identifier les vulnérabilités
- Identifier les dommages potentiels

Ce qui suppose

- d'être sensibilisé et vigilant
- savoir repérer une sensibilité
- savoir évaluer le « prix » attaché à la confidentialité d'une donnée sensible

Si possible dans le cadre général d'une étude de risques (qui s'inscrit normalement dans la PSSI de l'unité)

Mais aussi lors de besoins ponctuels (acquisition de réflexes) - e.g. transmissions -



COMMENT ?

Définir un dispositif de protection, global et cohérent (cf. analyse de risques)

**Y inclure le recours au « chiffrement »
⇒ en tant qu'**outil** « nécessaire » mais
non « suffisant »**

⇒ et inséparable d'un **protocole de mise
en oeuvre**



Le chiffrement...attention « danger »

Risque de perte de données pour l'agent

Risque de perte de données pour le service

Pas de sécurité absolue

Niveau de sécurité très variable, selon l'algorithme mais surtout les conditions de mise en oeuvre



Le chiffrement...un cadrage indispensable

Nécessité de recommandations spécifiques (politiques, techniques, organisationnelles)

fondées sur des appréciations techniques et organisationnelles (pertinence, fiabilité, facilité de déploiement des solutions logicielles...)

et sur des tests de terrain mettant en situation la mise en œuvre de solutions de chiffrement (approche expérimentale)

« ils l'ont fait, vous pouvez le faire ! »



La démarche retenue au CNRS

Imposer le résultat (protection des données) et non le moyen (tel outil...)

⇒ Pas de « modèle » imposé, donc pas de déploiement unique et centralisé au CNRS

N'imposer le résultat que si l'on peut offrir des moyens

⇒ recommandations



La démarche retenue au CNRS

Ce qui a été fait :

Identification du besoin

Identification de types de solutions logicielles

Tests sur le terrain (ZoneCentral)

Cf travaux INRIA, puis UREC et groupe JEANNIN

Sensibilisation et recommandations générales

- n° 55 et 62 de Sécurité Informatique

- Note de « Recommandations » (François Morris), en ligne sur le site FSD



La démarche retenue au CNRS

Ce qui reste à faire

- **des tests de terrain (opérations pilotes)**
- **les recommandations « opérationnelles »**
 - + en continu : actions de sensibilisation et de suivi



Pourquoi des opérations pilotes ?

- **tester la faisabilité technique et organisationnelle**
- **formuler des recommandations crédibles**
- **offrir des références concrètes**
- **disposer au CNRS d'un échantillon d'experts formés au travers de ces expériences**



Pourquoi des opérations pilotes

Les expériences doivent être représentatives des différents cas de figure possibles :

- **systèmes d'exploitation Windows, Mac, Linux, Unix**
- **environnements de travail divers (labos, DR, Siège...)**
- **chiffrement de surface de flottes de portables**
- **chiffrement de répertoires de postes et serveurs**
- **chiffrement de supports amovibles**
- **chiffrement de transmissions internes et externes (vis-à-vis de partenaires extérieurs)**



Deux opérations pilotes en parallèle

1) Chiffrement « systématique » de surface des nouveaux portables (opération menée par l'IN2P3)

Pilotes : François MORRIS et Thierry MOUTHUY

2) Chiffrement spécifique de données sensibles

Pilote : Bernard PERROT

+ cadrage d'ensemble et suivi par un groupe de travail « chiffrement »

Délais : tests terminés juin 2009 et bilans septembre 2009



Vos contacts au service du FSD

Protection du patrimoine scientifique	Jean-Luc Toffart mail : jean-luc.toffart@cnrs-dir.fr tél : 01 44 96 41 5
Sécurité des systèmes d'information	Robert Longeon mail : robert.longeon@cnrs-dir.fr tél : 01 44 96 48 76 + <i>François MORRIS</i> mail : francois.morris@impmc.jussieu.fr tél : 01 44 27 37 85
Missions à l'étranger – Formations - Habilitations	Josiane Pauchont mail : josiane.pauchont@cnrs-dir.fr tél : 01 44 96 41 84
Secrétariat technique	Christine Pierre mail : christine.pierre@cnrs-dir.fr tél : 01 44 96 41 85
Le Fonctionnaire de Sécurité de Défense	Joseph Illand mail : joseph.illand@cnrs-dir.fr tél : 01 44 96 41 88

Site Web

<http://www.sg.cnrs.fr/FSD/default.htm>

Mail

Fonc-Def-Sec@cnrs-dir.fr