

Sécurisation des données par le chiffrement

Journée Capitoul sur la mobilité
26 Avril 2007

Stéphane Calgaro (DR14)
Xavier Jeannin (UREC)



DR14 – pilote chiffrement - 1/19

Plan:

➤ **Généralité sur le chiffrement:**

- ✓ objectif et besoins
- ✓ principe
- ✓ recouvrement

➤ **Le logiciel Zone Central:**

- ✓ principe
- ✓ recouvrement

➤ **L'opération pilote:**

- ✓ les participants
- ✓ architecture mise en place
- ✓ retour d'expérience

➤ **Conclusion**



Généralité sur le chiffrement - objectif et besoins -

Éviter le vol de données dans un contexte de recherche:

- Lors de déplacement, typiquement sur un portable.
- Tout au long de la vie de la donnée.
- Poste fixe, Portable, Clé USB, sauvegarde.

Diversité des besoins:

- Une classification des laboratoires allant de sensible à régime ordinaire.
- Données classifiées.
- Contrats industriels.
- Données nominatives (Médicale).
- Différents systèmes d'exploitation.

Premier objectif : les postes de travail personnels, principalement des ordinateurs portables, au CNRS.



Généralité sur le chiffrement

- principe -

Type de chiffrement:

- **Chiffrement de file system.**
- **Chiffrement de surface.**

Une clé symétrique pour le chiffrement pour des raisons de performance.

Une clé d'accès qui libère la clé de chiffrement : mot de passe, bi-clés, certificat numérique.

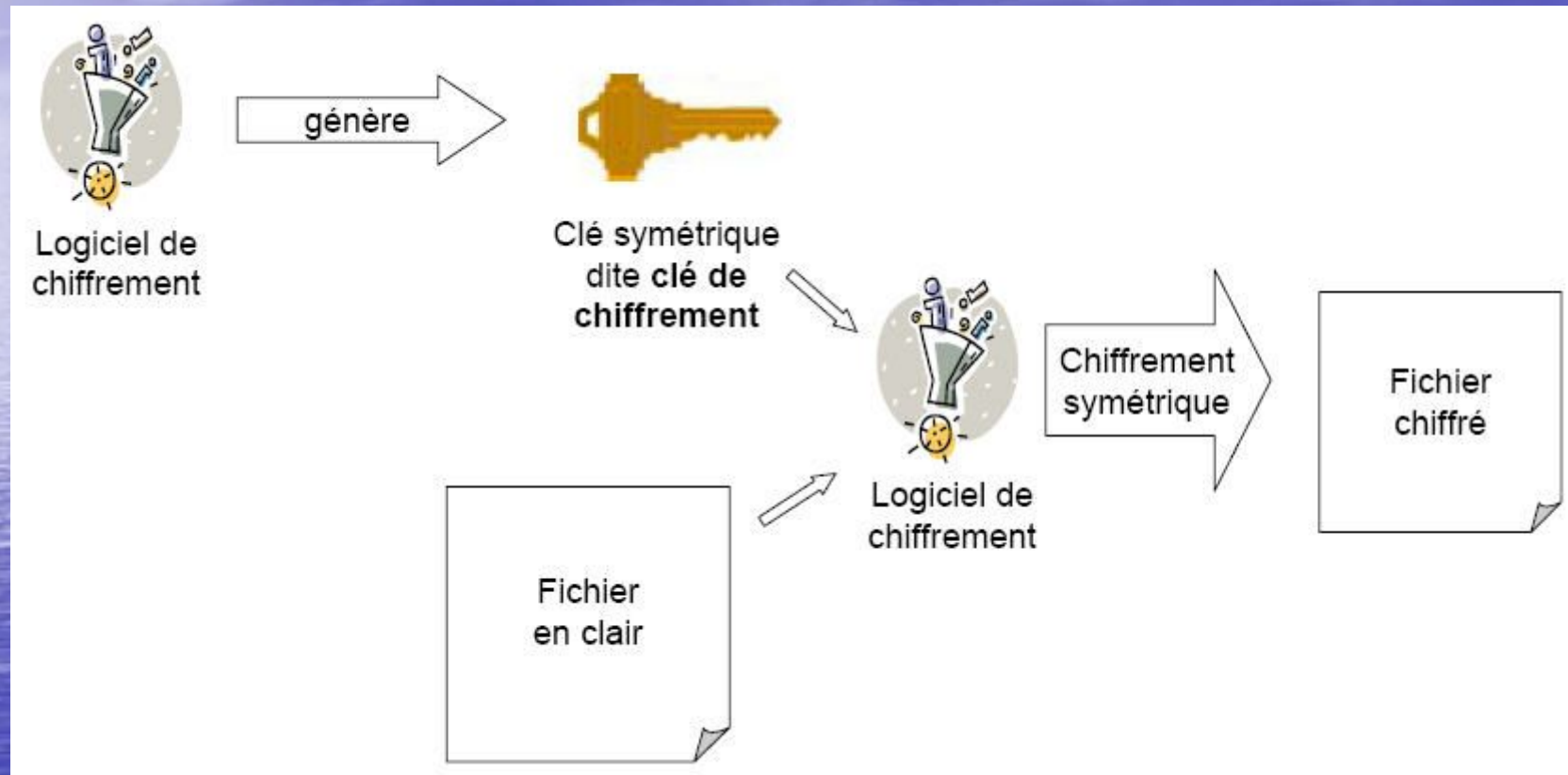
La gestion de la distribution des clés d'accès:

- **Le stockage des clés d'accès utilisateurs.**
- **Token, fichier PKCS12.**



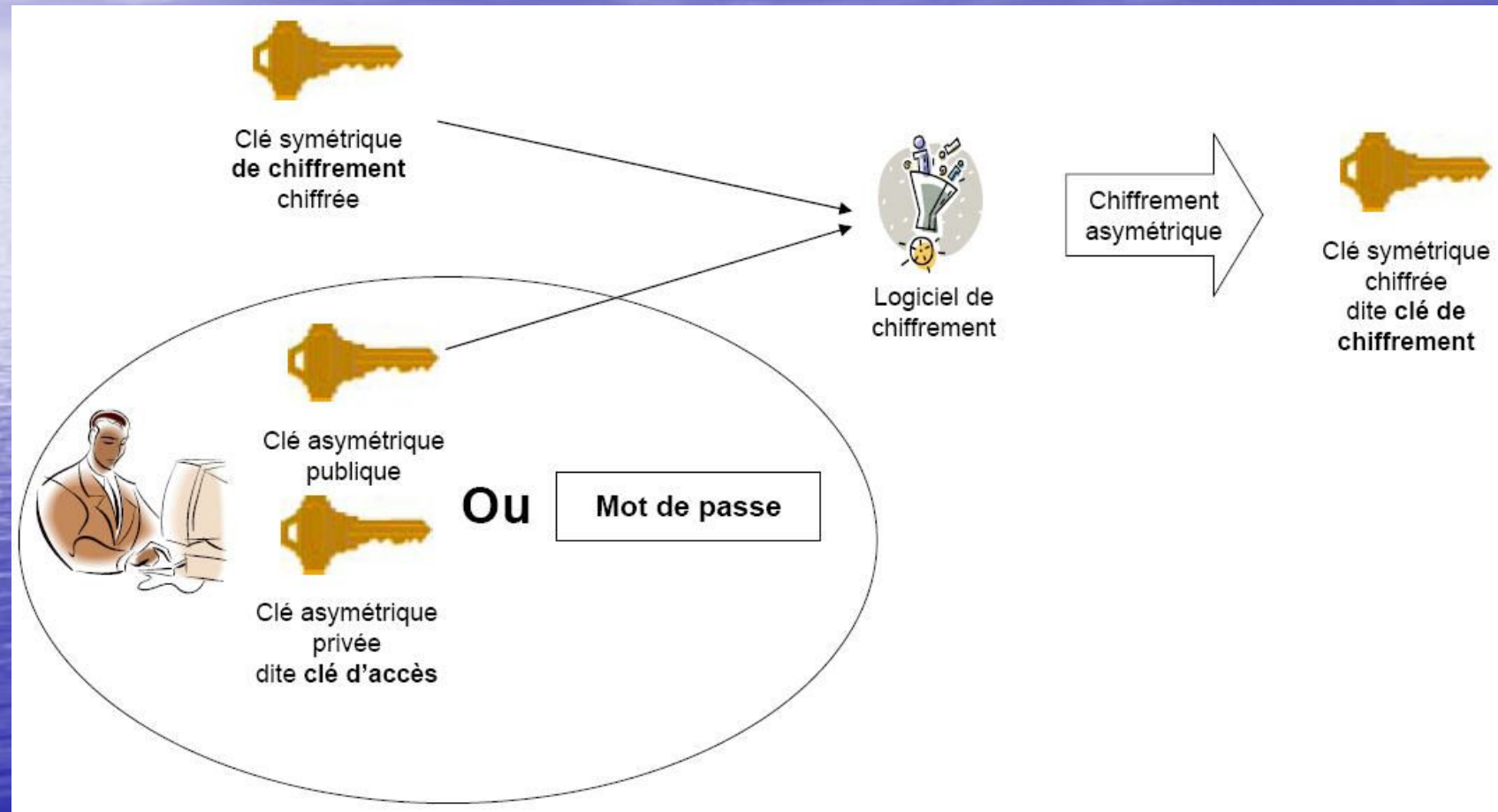
Généralité sur le chiffrement

- principe -



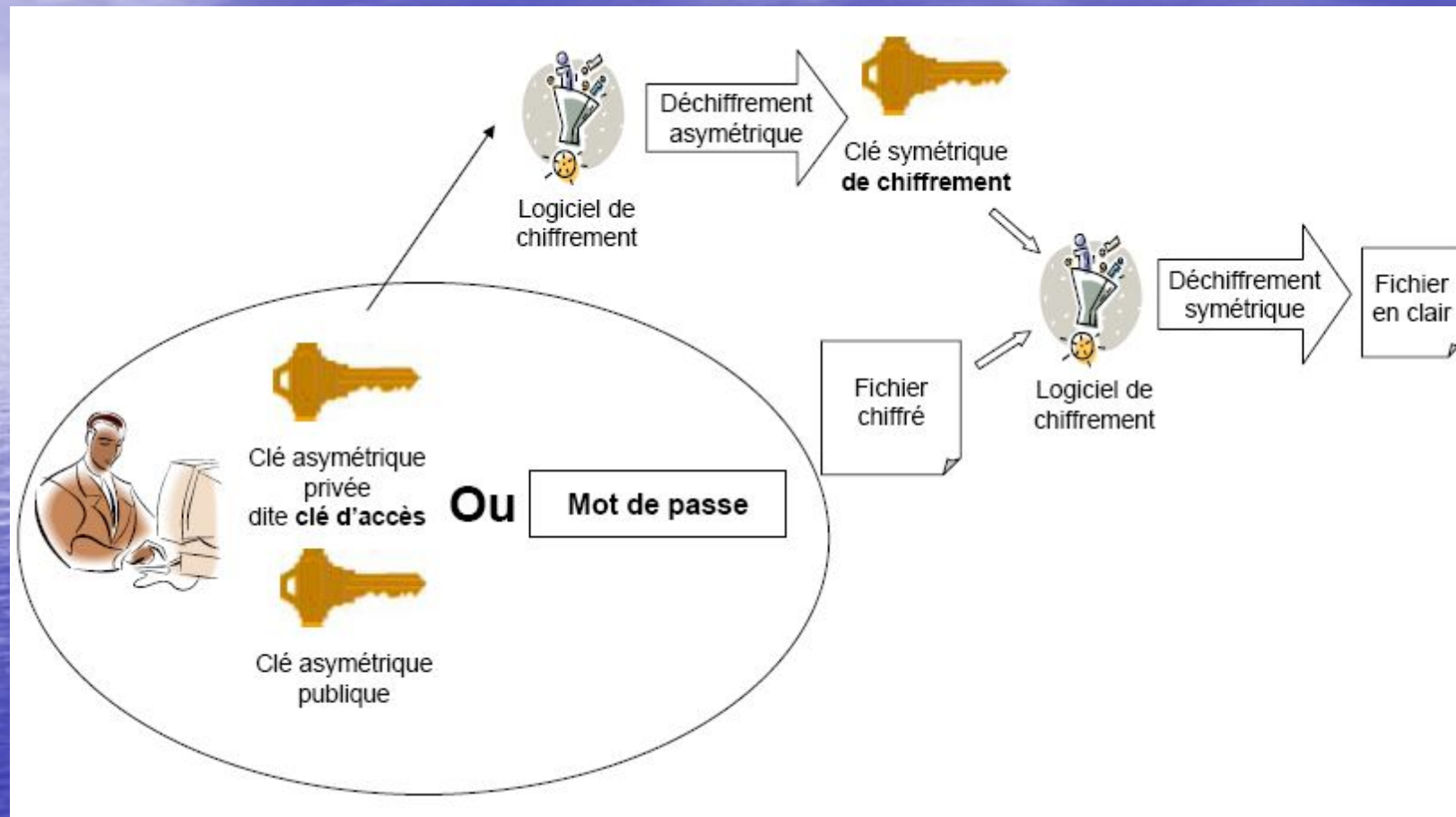
Généralité sur le chiffrement

- principe -



Généralité sur le chiffrement

- principe -



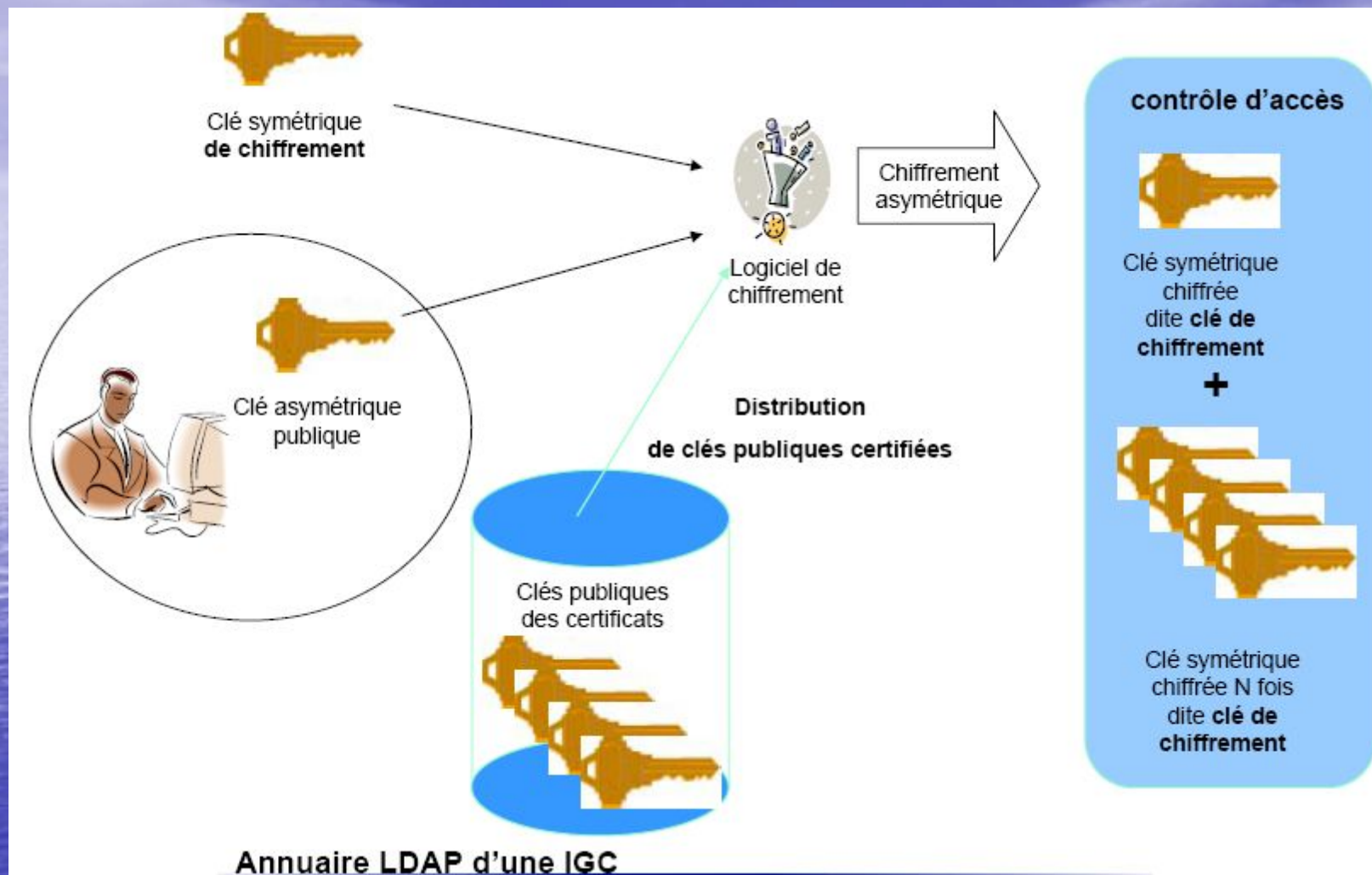
Généralité sur le chiffrement - recouvrement -

Le but du recouvrement:

- **Restaurer les données en clair, voire accéder à la machine.**
- **Récupérer les données et non les clés déchiffrement ou d'accès**
- **Palier à une perte de clé, répondre à une requête interne ou externe**



Généralité sur le chiffrement - recouvrement -



Généralité sur le chiffrement - recouvrement -

Séquestre de tous les secrets !
Personne de confiance habilitée !

Recouvrement : chiffrement avec un autre secret ou le secret d'un autre utilisateur:

- Avec un mot de passe de secours (solution centralisée)
- Par le logiciel en vue d'utiliser un système Challenge / Response service d'assistance(solution centralisée)
- Chiffrer avec la clé d'autres utilisateurs = accès multiple

Clés pour le recouvrement:

- Dans une IGC les clés publiques sont certifiées, distribuées facilement et peuvent permettre la mise en place d'un recouvrement.
- Avec des clés ou des certificats d'une durée longue qui réaliserait le recouvrement
- Usage d'un token (clé non exportable)

Défini par la politique de sécurité: niveau local, national



Zone Central - principe -

Zone Central, éditeur Prim'X

Chiffrement de file system

Fonctionne par zone de chiffrement (un répertoire).

Accepte comme clé d'accès :

- **Des mots de passe.**
- **Des certificats (gestion des révocations).**
- **De mot passe de secours pour le dépannage à distance.**
- **Gestion par liste d'accès**
- **Supporte les tokens**

Intégration des stratégies dans un domaine Windows (GPO) et en local

Possibilité de chiffrer toutes les données modifiables d'un utilisateur (pseudo poste complet).



Zone Central
- recouvrement -

- Avec un mot de passe de secours (solution centralisée):
oui, mais nécessite le séquestre de la liste d'accès de l'utilisateur.
- Par le logiciel en vue d'utiliser un système Challenge / Response service d'assistance(solution centralisée):
non disponible
- Chiffrer avec la clé d'autres utilisateurs = accès multiple:
*oui, rôles « recouvrement » prévus et implémentés.
Par défaut, ouverture de zone interdite aux accès recouvrement.*



L'opération pilote - Les participants -

UMR5044: CERTOP - Département SHS – 75 personnes.
Tests effectués par Joël Courant .

UMR5187: CESR - Département MPPU - 150 personnes.
Tests effectués par Cédric Hillebrandt

UMR5604: GREMAQ - Département SHS - 120 personnes.
Tests effectués par Erwan Bossis

UMR5502: IMFT - Département ST2I - 190 personnes.
Test effectués par Henri Ipinazar et Gilles Martin

UMR5563: LMTG - Département MPPU - 180 personnes.
Test effectués par Philippe Azema

UMR5068: SPCMIB - Département SC - 60 personnes.
Test effectués par Frederic Rodriguez

UPR8001: LAAS - Département ST2I – 600 personnes.
Tests effectués par N.RAKOTOMAMPIONONA et J. LIBOUREL

MOY1400: Délégation Midi-Pyrénées - Moyens Communs - 100 personnes.
Tests effectués par R. Dartiguepeyron et S. Calgaro



L'opération pilote - contexte -

Coordination: R. Dartiguepeyron, X. Jeannin, S. Calgaro

- **Type de laboratoire très varié et formé sur les certificats.**
- **3 laboratoires sont classés ERR.**
- **Formation des ASR, des agents de recouvrement.**
- **Organisme fortement décentralisé, multi tutelle.**
- **Taille hétérogène des laboratoires.**
- **Parfois peu de moyen informatique.**
- **Peu de sensibilisation aux problèmes de confidentialité.**

Fin opération : 31 mars 2007

Rapport final de l'opération en cours de finalisation.



L'opération pilote - Architecture mise en place -

But: test du déploiement et de l'usage du produit in vivo.

Clé d'accès et de recouvrement sont des certificat numériques (validité: 5 ans) -> évolution de l'IGC CNRS.

En téléchargement (via [https DR14](https://dr14.cnrs.fr)):

- Ressources documentaires et organisationnelles (supports de formation, présentations connexes)**
- Certificats de recouvrement nationaux, régionaux et liste d'accès obligatoire (avec son hash)**
- Stratégie de paramétrage du produit**
- Informations diverses**

liste de diffusion mël gérée par la délégation.

Licences du produit prise en charge par le CNRS (UREC).

Accès illimité au support Prim'X



L'opération pilote - Architecture mise en place -

Liberté de déploiement pour les ASR.

Seuls 2 impératifs:

- MISE EN PLACE D'ACCES OBLIGATOIRE = recouvrement.

Recouvrement (4 a 6 certificats):



nouveau certificat de recouvrement au bout de deux ans et demi (*pour avoir un chevauchement*)

- Séquestre des listes d'accès



L'opération pilote - Retour d'expérience -

- Des besoins mais peu de demande
- Besoin de sensibilisation au niveau des directeurs:
réticences voire refus à la mise en place du produit de chiffrement !
- Déploiement sans difficulté dans les laboratoires
- Produit considéré comme «apte au service»
- Logiciel facile à prendre en main.
- Le paramétrage n'est pas forcément évident.
- Bonne intégration dans Windows surtout dans un domaine Windows (GPO).
- Surveiller la comptabilité avec d'autres logiciels (antivirus, graveur de CD).
- Des exemples chiffrement intégral de chaînes de traitements scientifiques de l'information entièrement
- Pas de différence sensible de temps de traitement
- Tous les OS ne sont pas couverts



Conclusion

Le chiffrement est nécessaire dans les organismes de recherche

Le chiffrement va se répandre rapidement

Le chiffrement est relativement transparent et facile d'usage pour les utilisateurs mais il peut conduire à des situations difficiles

Le chiffrement doit s'adapter à l'organisme

Son déploiement doit être encadré et accompagné:

- **Organisation doit être définie : procédure de recouvrement**
- **Choix du logiciel**
- **Sensibilisation**
- **Un mauvais déploiement peut être fortement contre productif.**
- **Offrir une assistance et un support.**



Merci de votre attention

Questions ?

