ZoneCentral 2.5

Intégrer le chiffrement et faciliter son intégration dans votre entreprise !

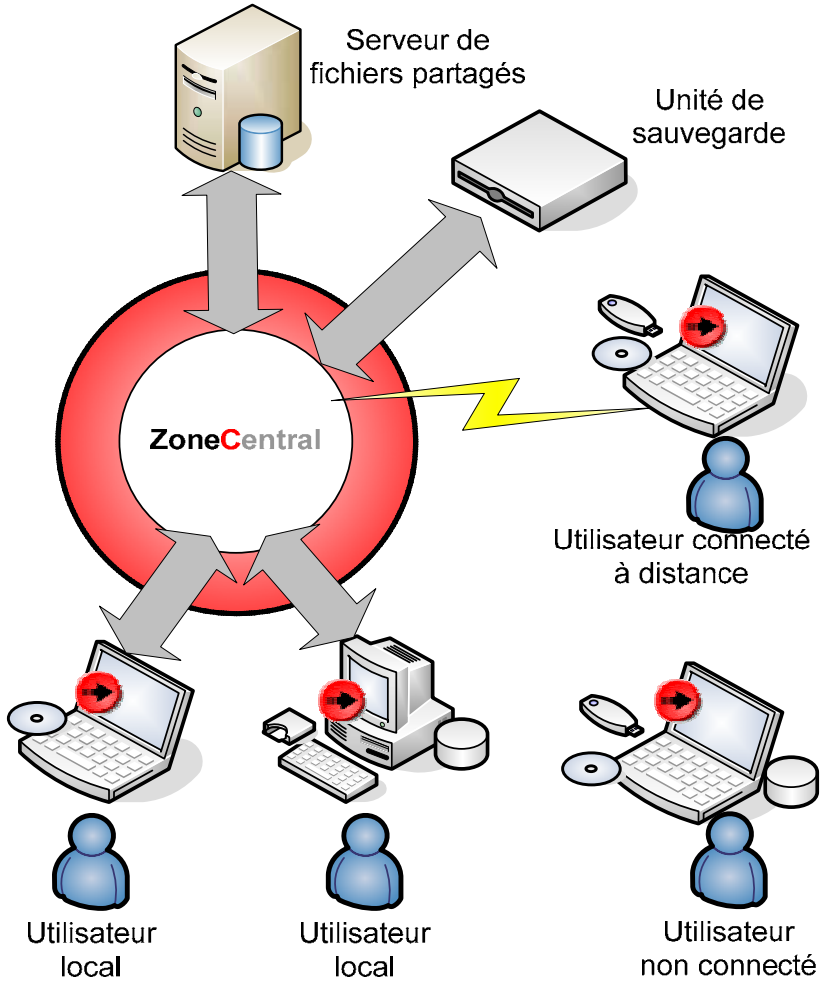
Prim'X TECHNOLOGIES

Sommaire

- ZoneCentral - le chiffrement ‘in-place’
- Les Zed! - conteneurs sécurisés
- Sécurité du poste de travail

Chiffrement « in-place »

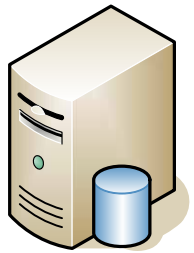
- **ZoneCentral s'installe et s'exécute sur les postes de travail**
- **Chiffrement des fichiers là où ils sont : *Poste de travail, Serveur, Support amovible***
- **Exécution 'à la volée' du chiffrement/déchiffrement**
- **Postes de travail Windows 2000, XP, 2003**
- **Tous types de serveurs : Unix, Novell, Windows, …**



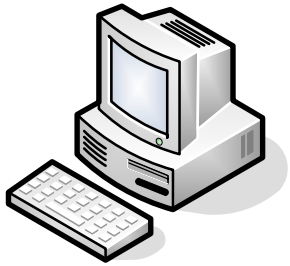
Cas d'application : confidentialité des fichiers

- **Protection des flottes de postes mobiles** (perte, vol,…)
- **Protection des postes fixes** (droit d'en connaître, vol du disque dur, intrusion,…)
- **Protection des partages de fichiers sur serveurs** (droit d'en connaître,…)
- **Protection des supports amovibles** (sauvegardes, sticks mémoire USB,…)

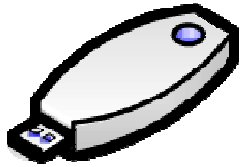
Portables



Serveurs de fichiers



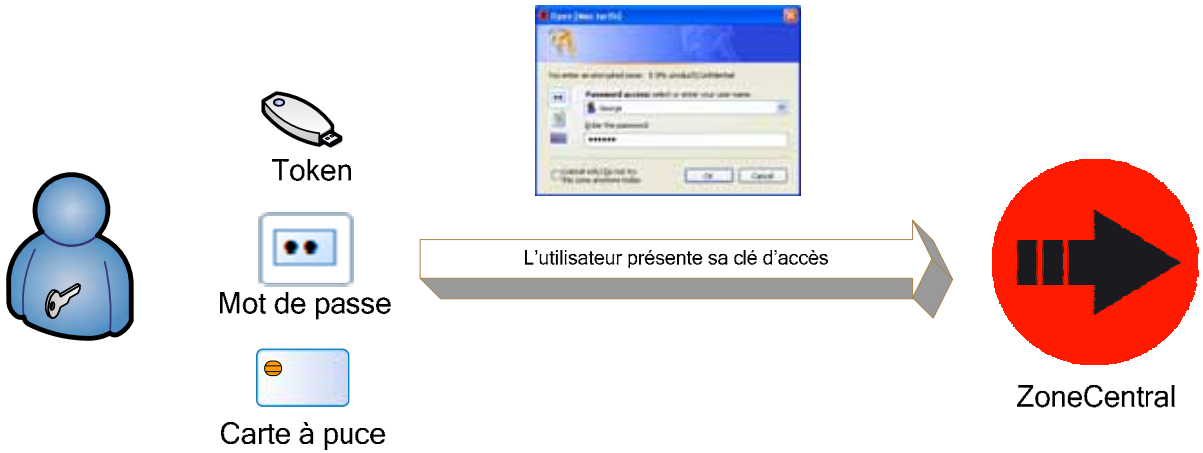
Postes fixes



Supports amovibles

Les concepts (1)

- **Produit transparent pour l'utilisateur**

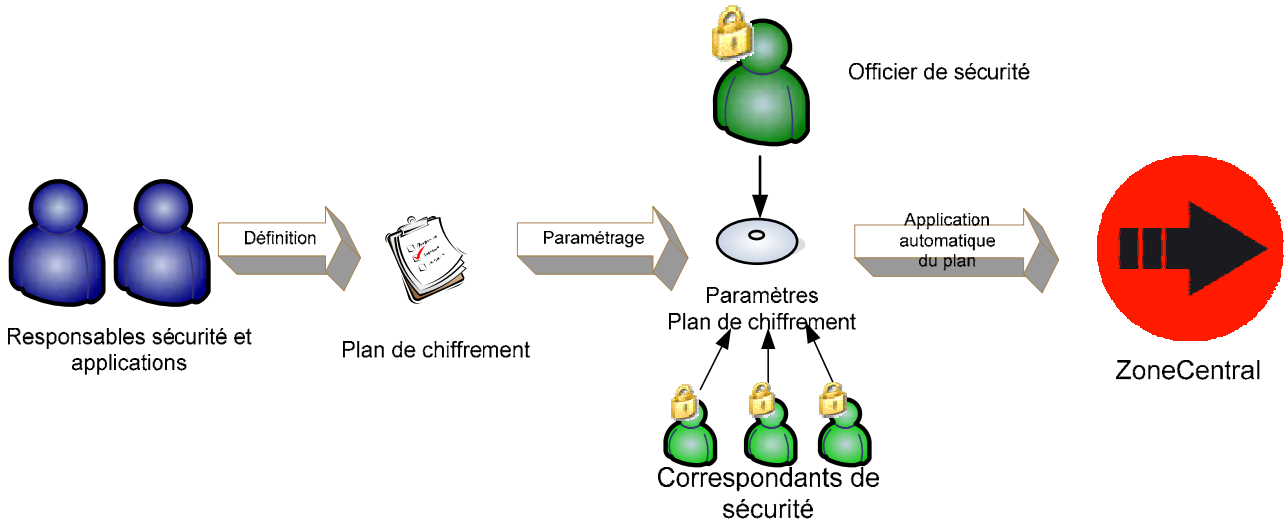


L'utilisateur présente sa clé qui peut être un mot de passe ou un bi-clé RSA hébergé par une carte à puce ou un token USB… C'est la seule interaction de l'utilisateur avec le produit. Le chiffrement/déchiffrement des fichiers se fait ensuite automatiquement et à la volée lorsque l'utilisateur y accède.

La présentation de la clé peut se faire via un écran ZoneCentral ou bien avec une carte à puce ou un token au login Windows

Les concepts (2)

- **Possibilité de plan de chiffrement défini et contrôlé par l'entreprise, appliqué systématiquement par ZoneCentral**

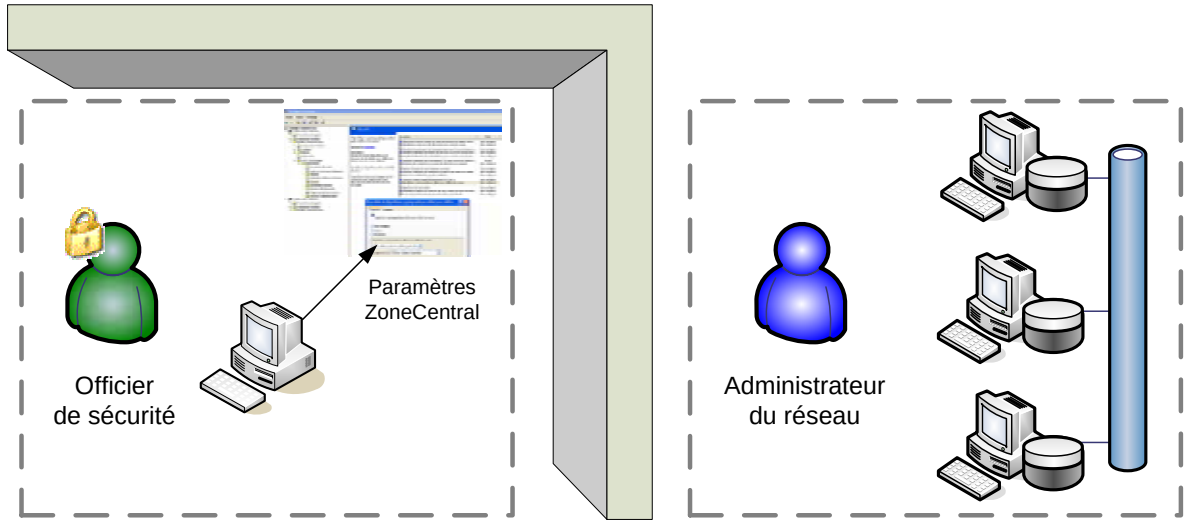


- Les responsables des données (officier de sécurité, responsable d'application, dirigeants…) spécifient le plan de chiffrement i.e. pour l'essentiel ce qui doit être chiffré, sur les postes de travail et les serveurs. Le plan désigne aussi les clés de recouvrement, les correspondants de sécurité, etc.
- Le plan de chiffrement est traduit en paramètres par l'officier de sécurité et ses correspondants.
- ZoneCentral applique automatiquement le plan de chiffrement qui lui est communiqué

Les concepts (3)

- **Séparation possible des tâches d'administration de la sécurité d'une part et d'administration du réseau et postes de travail d'autre part**

  Avec ZoneCentral
  - Le système est toujours en clair … donc toujours accessible
  - Les données de l'utilisateur sont chiffrées (en totalité ou de façon sélective)



L'officier de sécurité administre le chiffrement des fichiers sur les postes de travail et les serveurs.

L'administrateur du réseau et des postes de travail effectue son travail normalement sans aucune contrainte due au chiffrement puisque le système est en clair.

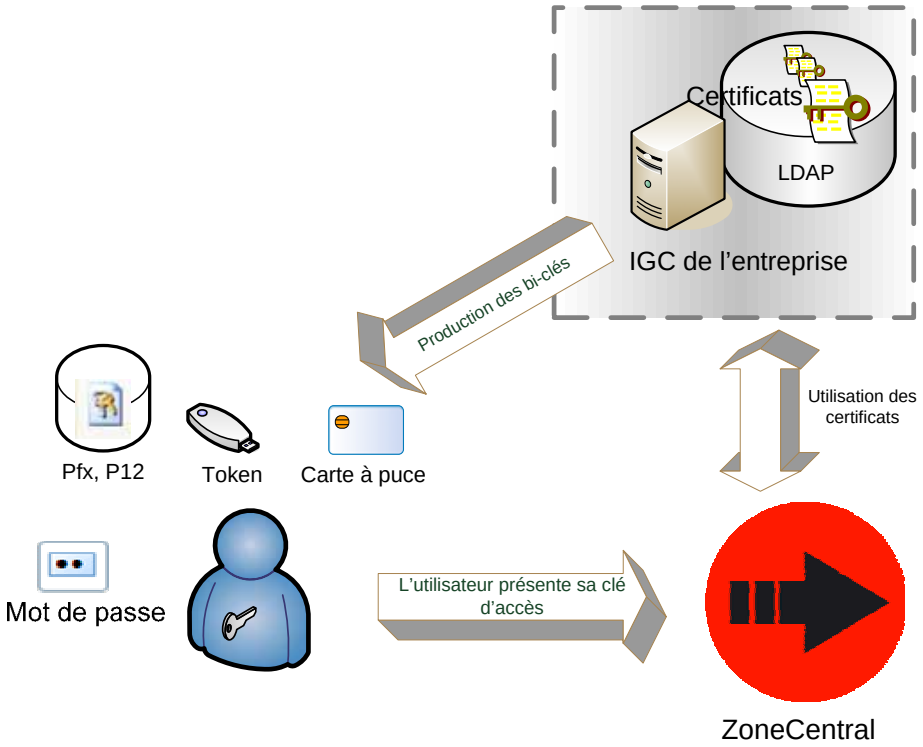
Cette organisation est particulièrement intéressante lorsque la bureautique fait l'objet d'une prestation d'outsourcing (interne ou externe)

Les concepts (4)

- **Indépendant des IGC**

  ZoneCentral est un ***produit d'application*** de l'IGC ;
  Il utilise les clés et les certificats produits par l'IGC de l'entreprise

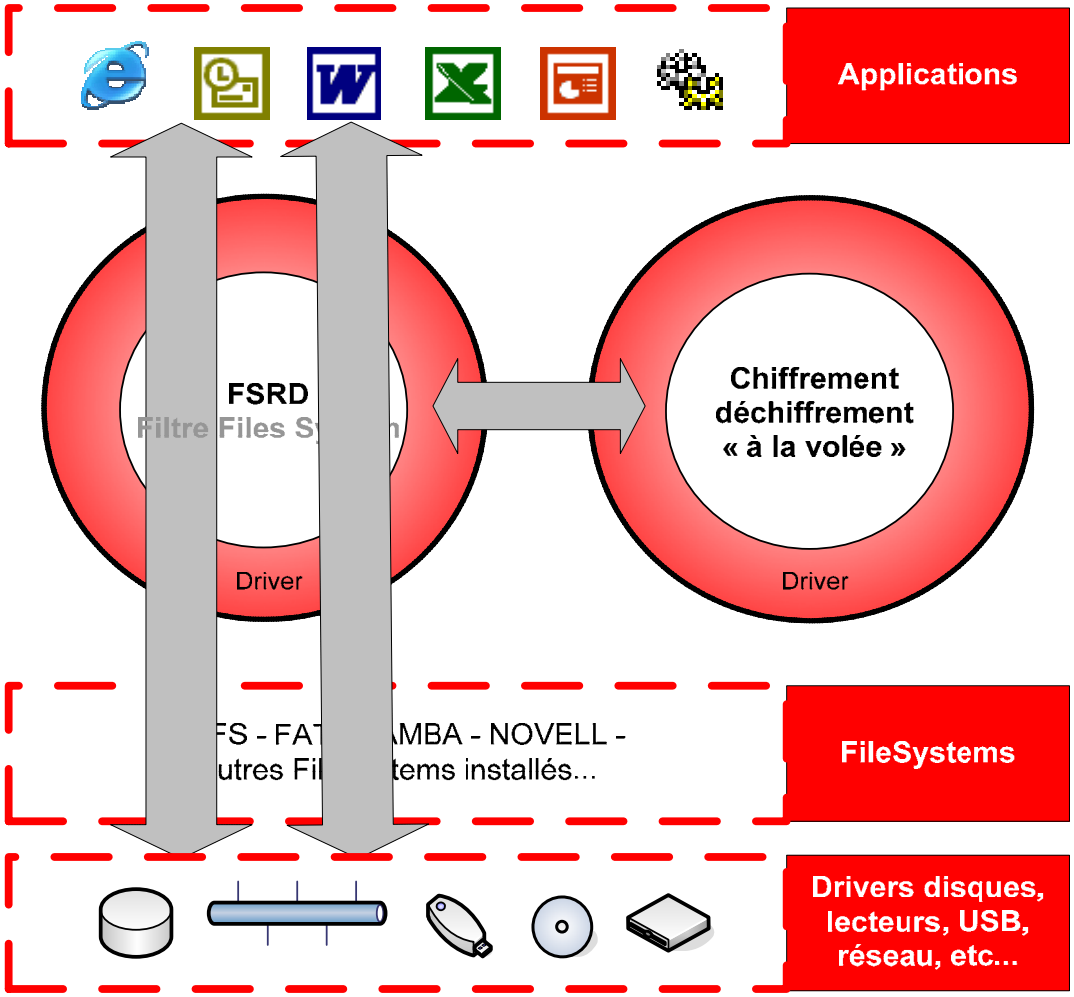
- **ZoneCentral fonctionne aussi sans IGC avec des mots de passe**



ZoneCentral peut utiliser simultanément des mots de passe et des clés RSA sur des supports de différentes marques (selon les utilisateurs ou les zones accédées)

Technologie

- Position en filtre au dessus des FileSystems
- Interception de toutes les I/O
- Exécution ‘à la volée’ du chiffrement/déchiffrement

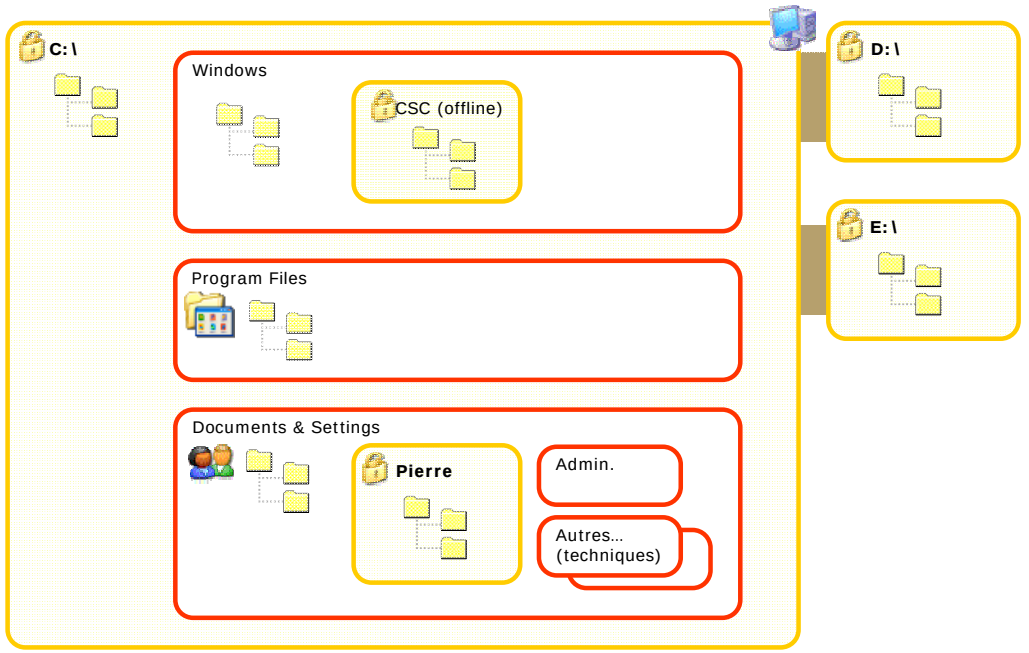


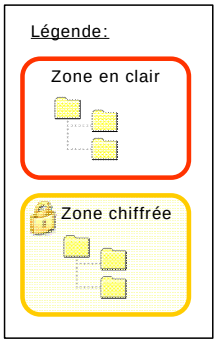
Que peut-on chiffrer avec ZoneCentral ? (1)

- **ZoneCentral chiffre des zones**
- **zone = dossier et tout ce qu'il contient sur N niveaux**

exemples de zones sur le poste de travail (fichiers personnels)

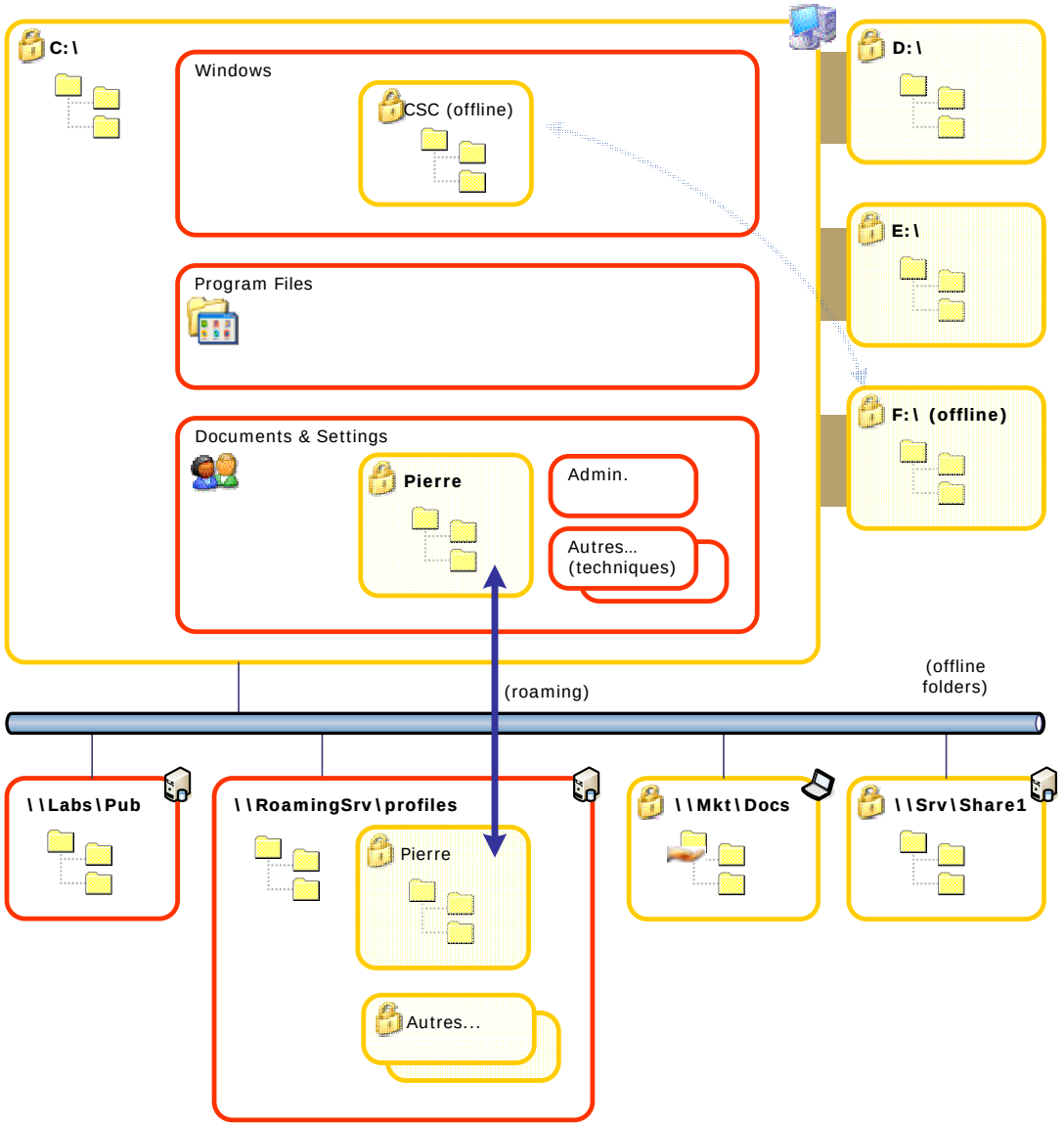
- Le bureau est chiffré
- Le cache internet est chiffré
- Le dossier « Mes documents » est chiffré
- Les fichiers temporaires sont chiffrés
- Le Swap est chiffré





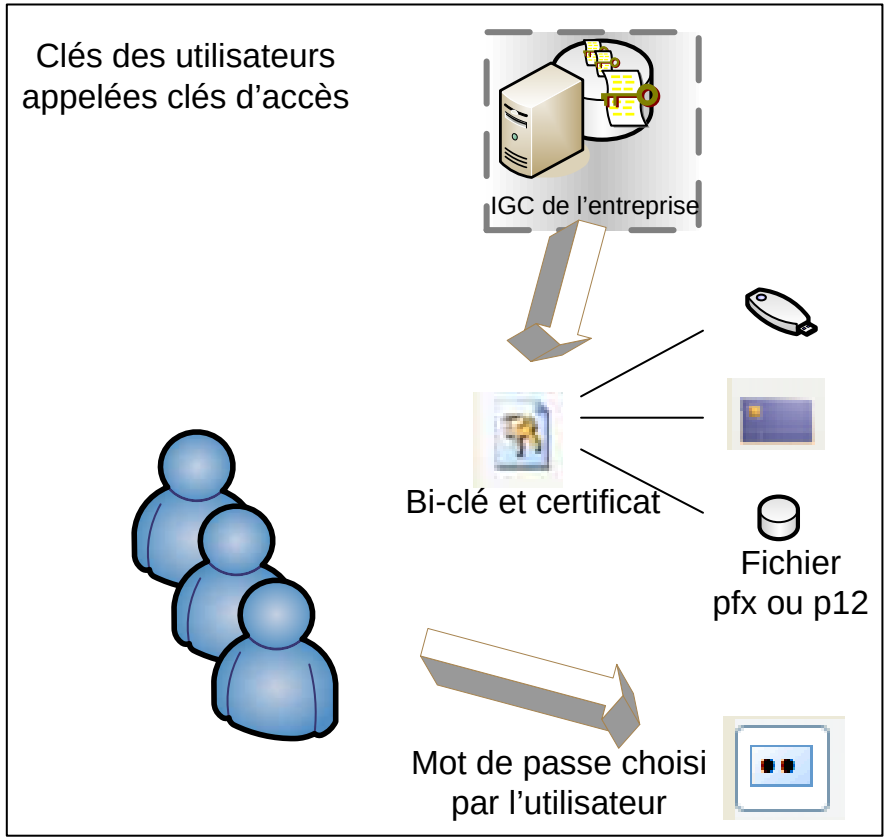
Que peut-on chiffrer avec ZoneCentral ? (2)

- **Les fichiers - partagés ou non - sur les serveurs peuvent être chiffrés**
- **Les profils itinérants (roaming) peuvent être chiffrés**
- **Les fichiers synchronisés (fichiers off-line) peuvent être chiffrés sur le poste de travail et le serveur**
- **Les sauvegardes du poste de travail peuvent être chiffrées**
  (outil de sauvegarde fonctionnant en mode raw)



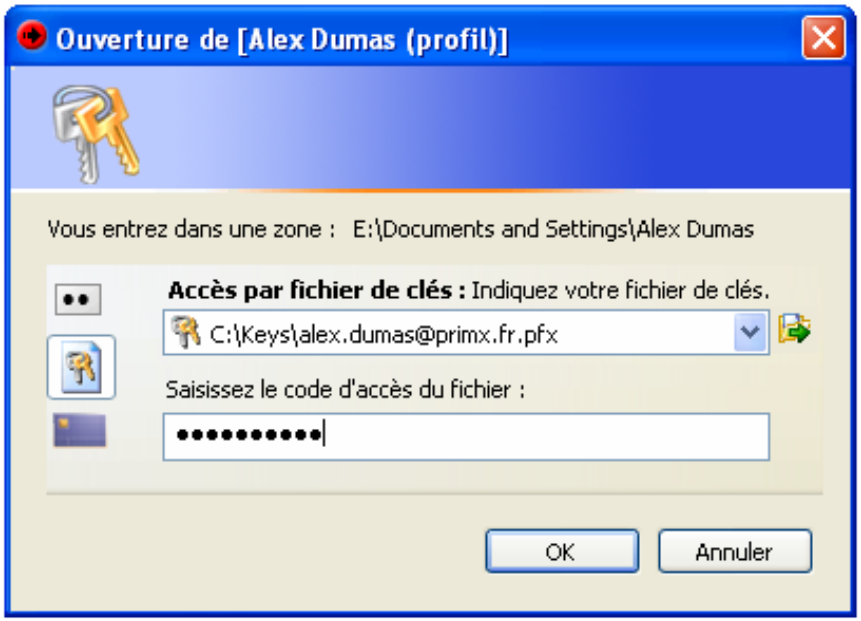
Clés et porte-clés des utilisateurs

- **la clé d'accès de l'utilisateur peut être un bi-clé RSA ou un mot de passe.**
- **gestion de porte-clés RSA de différentes natures**
  - Fichiers .pfx, .p12,
  - Carte à puce, token USB
  - CSP

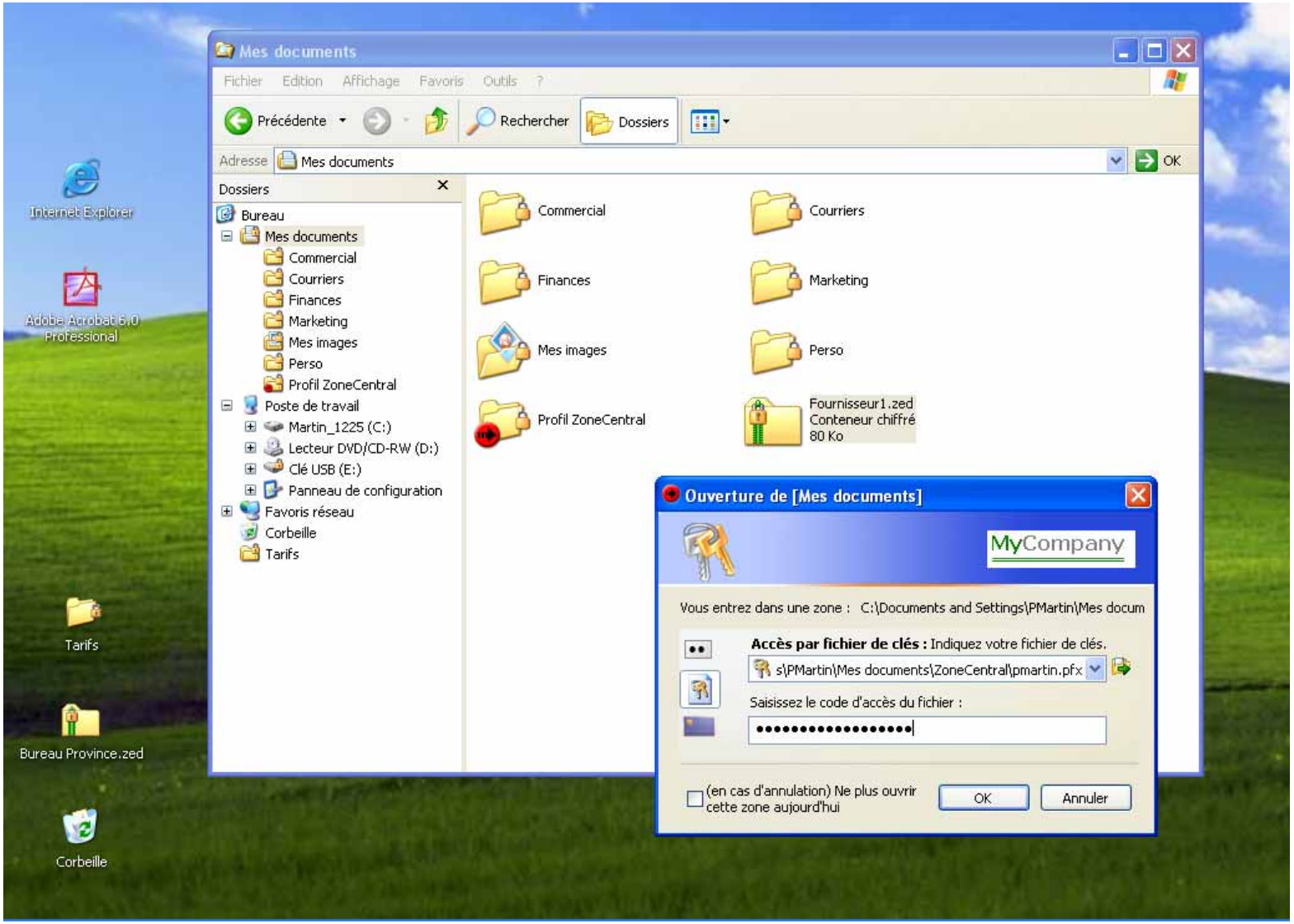


Fournir une clé d'accès

- **Apparaît lors du premier accès à un fichier situé dans une zone chiffrée**
- **Possibilité d'utiliser la technologie CSP de Microsoft**



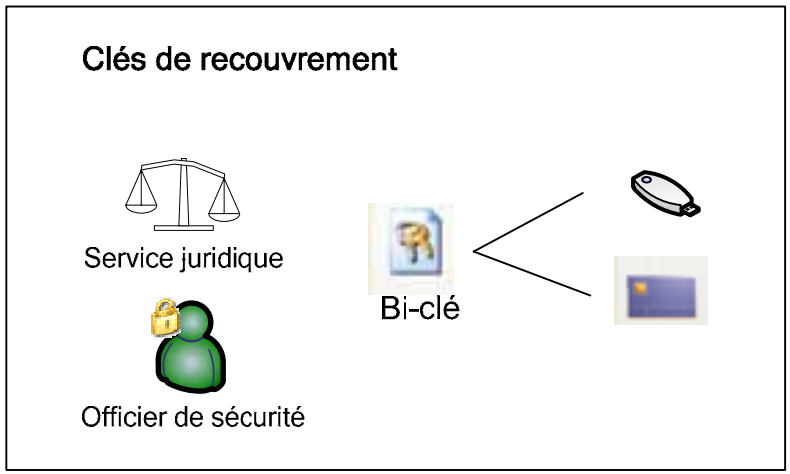
Ce que voit l'utilisateur



Clés de recouvrement

- **Clés de recouvrement**
  - Plusieurs clés possibles
  - Appliquées automatiquement par ZoneCentral

- **Mot de passe de secours**
  - Dédié à un utilisateur ou à un poste
  - Permet le dépannage de l'utilisateur à distance en cas de perte de sa clé d'accès
  - Recouvre les fichiers du poste de travail de l'utilisateur



Clés de chiffrement

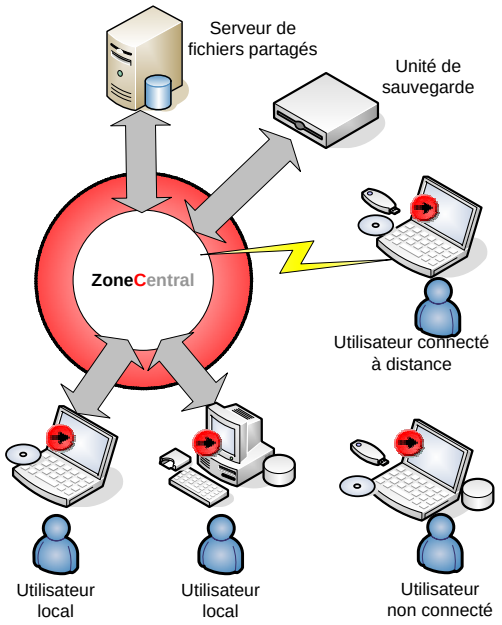
- **Les clés de chiffrement de fichiers sont des clés symétriques de type AES, DES, ou 3DES**

- **Nominalement se sont des clés AES 256 bits**

Clés symétriques de chiffrement des fichiers
(AES 256)
Tirées aléatoirement par ZoneCentral

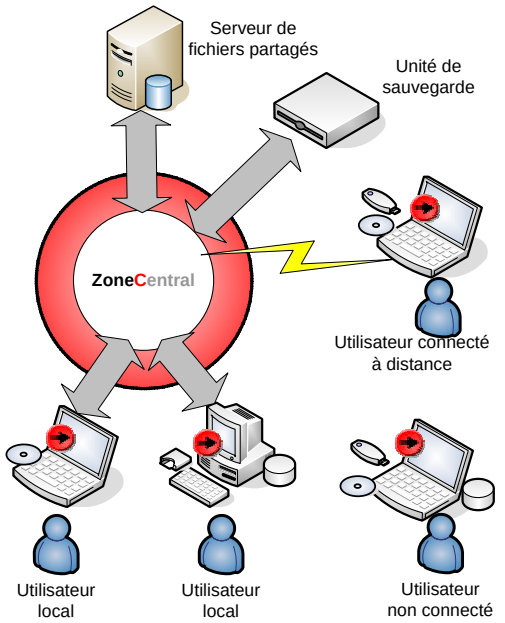
Sécurité de l'environnement

- **Effacement automatique à la volée** (sans intervention de l'utilisateur) **de tous les fichiers supprimés** (wiping par surcharge)**, y compris les fichiers temporaires**
- **Chiffrement du swap du poste de travail**
- **Anti-keylogger pour la saisie des mots de passe**



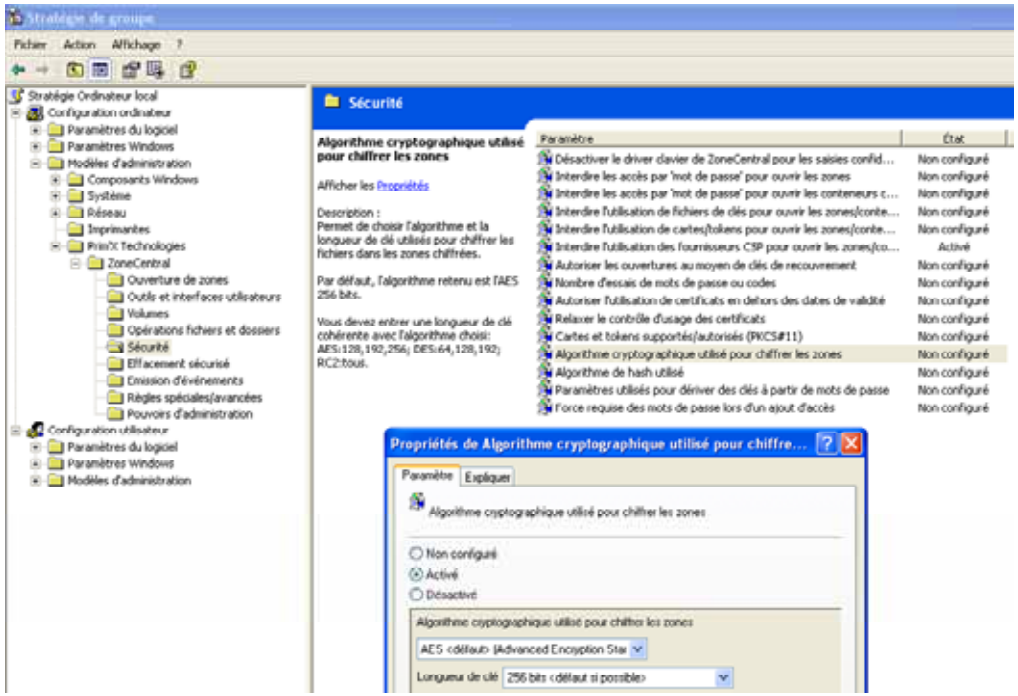
Cryptographie

- **Cryptographie renforcée implémentée sous forme de driver**
- **Possibilité de composants cryptographiques externes (matériels ou logiciels compatibles PKCS#11)**
- **Algorithmes : 3DES, AES (128 à 256 bits), et RSA (1024 à 4096 bits)**
- **Technologies PKCS#1, PKCS#5, PKCS#11, compatible PKIx**
- **Compatible avec les cartes à puces et tokens des principaux industriels.**



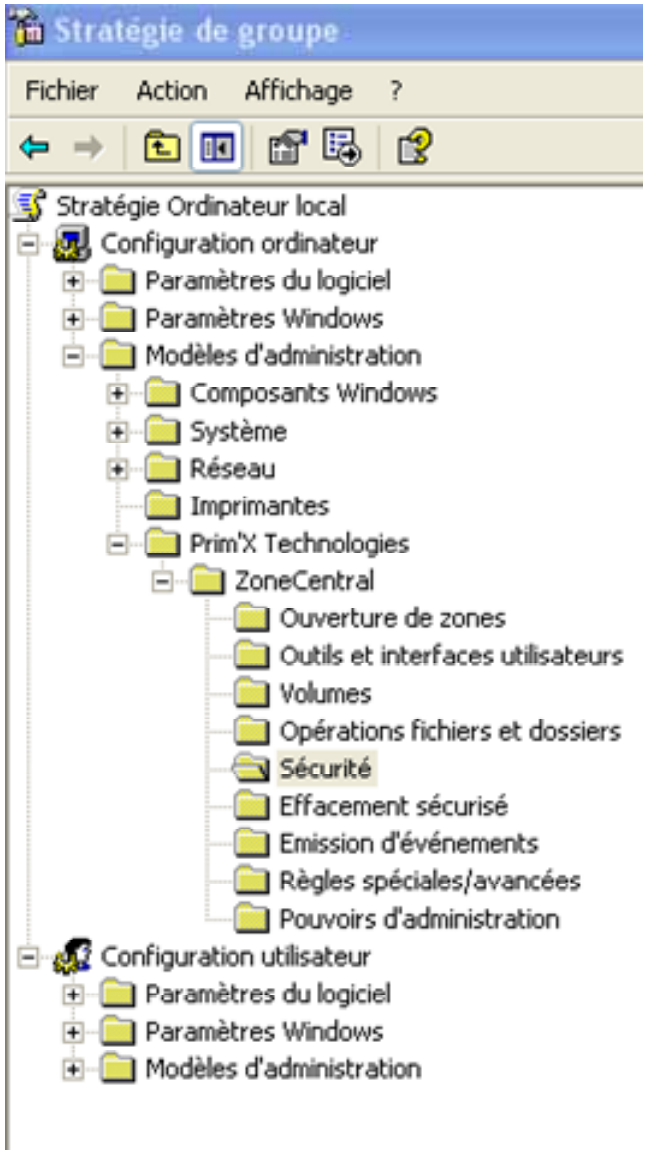
Le Plan de chiffrement

- Désigne les zones chiffrées sur le poste de travail
- Désigne les accès obligatoires (mandatory)
  - Clé(s) Officier Sécurité
  - Clé(s) de recouvrement
- Définit les délégations de droits d'administration
- Définit les paramètres du produit (algorithmes, longueur de clé, et tous les paramètres d'environnement…)
- Désigne l'emplacement des fichiers journaux
- Etc.



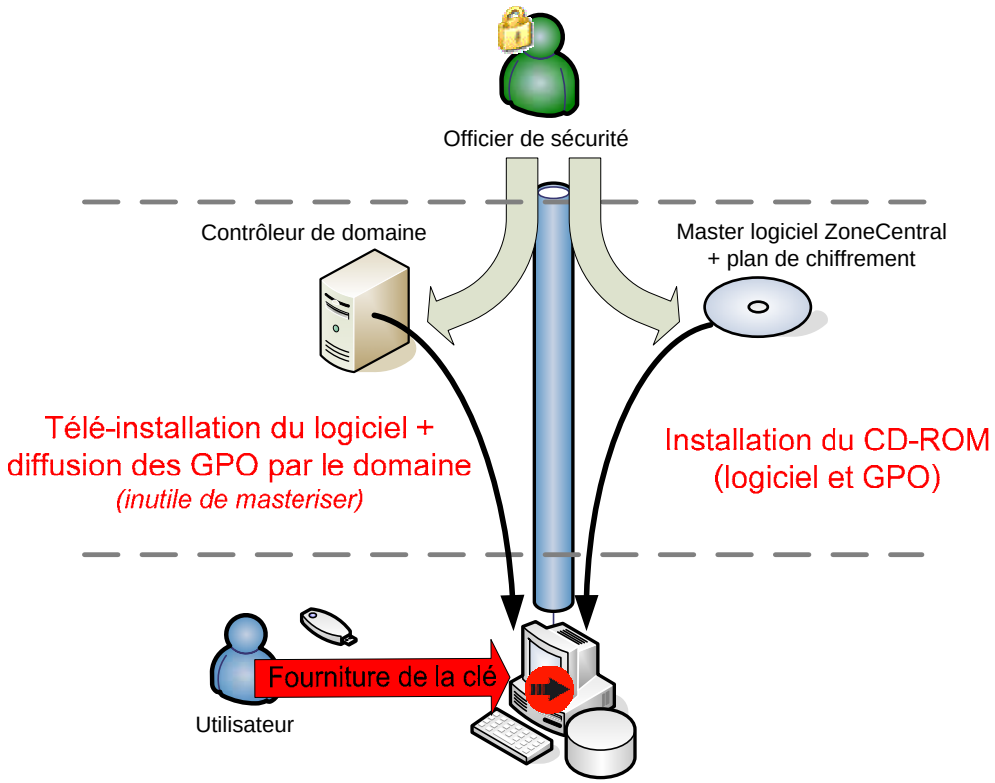
Paramétrage du Plan de chiffrement via des Policies de Windows

- Utilisation des GPO Windows, avec un modèle d'administration ZoneCentral
- Policies définissables en local ou en domaine (mécanisme de diffusion des serveurs Windows)
- Masterisation possible de Policies prédéfinies pour application locale (si hors domaine)



Un déploiement facile

- **Exemple de déploiement**
  - Préparation du Plan de chiffrement
  - Diffusion du logiciel et du Plan de chiffrement
  - A la première utilisation, application de la consigne de chiffrement

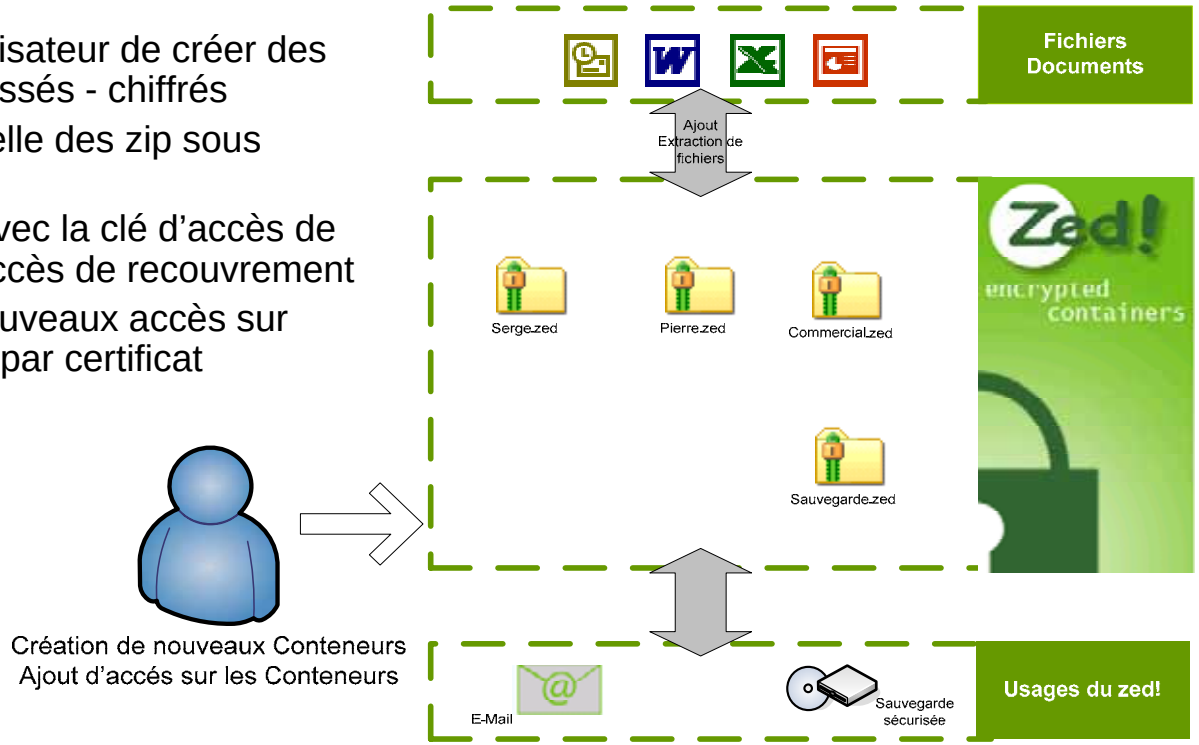


Exploitation

- **Contrôle des fichiers d'évènements**
- **Secours des utilisateurs ayant perdu leur clé d'accès**
- **Ajouts/retraits d'accès sur les zones partagées -** notion de correspondants de sécurité
- **ZoneCentral se charge de la ré-application automatique du plan de chiffrement à chaque démarrage**

Les conteneurs chiffrés

- La fonction Zed! permet à l'utilisateur de créer des conteneurs de fichiers compressés - chiffrés
- L'ergonomie est identique à celle des zip sous Windows XP
- Le conteneur est accessible avec la clé d'accès de l'utilisateur qui le crée et les accès de recouvrement
- L'utilisateur peut ajouter de nouveaux accès sur chaque conteneur par MP ou par certificat



Pour les postes non équipés de ZoneCentral, Prim'X fournit un package libre de licence : **Zed! Limited Edition** il possède toutes les fonctions de Zed! sauf les services de création de nouveaux conteneurs et d'ajout d'accès sur un conteneur existant.

Zed! Limited est disponible sous forme installable ou comme simple exécutable

Politique commerciale et support

- **Prospection directe - Ventes indirectes**
- **En France**
  - Réseau d'intégrateurs : *spécialisés - institutionnels - généralistes*
  - Réseau de distributeurs : *grossistes à valeur ajoutée - revendeurs*
  - Prestataires d'infogérance
- **A l'international**
  - Réseau d'importateurs « à valeur ajoutée » en 2006
- **Support**
  - Formation/support des intégrateurs
  - Prestations de conseil/consulting
  - Contrat de maintenance évolutive et support niveau 2
  - Rubrique Web « Prim'X Tools » : *Outils d'aide au déploiement en libre service*
- **Références**

Rappel des fonctionnalités - packages (1)

Chiffrement	ZoneCentral	ZC express
Chiffrement à la volée, de fichiers personnels sur unités locales ou amovibles	☑	☑
Chiffrement de fichiers partagés sur les unités locales, amovibles ou réseau (serveurs Windows,UNIX, Novell…)	☑	
Chiffrement automatique du swap	☑	☑
Conteneurs compressés-chiffrés pour échanges	☑	option
Chiffrement possible du cache des navigateurs (protection Intranet)	☑	☑
Chiffrement possible du profil utilisateur (bureau, mes documents, temporaires, cache Internet, …)	☑	☑
Chiffrement possible de postes ou de volumes entiers, y compris le volume système (sauf le système lui-même, pour permettre l'administration bureautique par un tiers)	☑	☑
Détection automatique des clés-mémoires USB avec proposition de chiffrement	☑	☑
Compatible roaming (profil chiffré) et dossiers chiffrés off-line	☑	☑
Fichiers temporaires chiffrés	☑	☑
Clés d'accès utilisateurs		
Accès par mots de passe (force contrôlable)	☑	☑
Accès par clés RSA sur porte-clés fichiers PFX/P12	☑	☑
Accès par clés RSA sur porte-clés cartes&tokens PKCS#11, conteneurs CSP	☑	option
Compatible PKI et LDAP	☑	☑
Gestion de groupes (listes d'accès)	☑	
Gestion de rôles (utilisateur, administrateur de zone, recouvrement, secours)	☑	☑

Rappel des fonctionnalités - packages (2)

Sécurité de l'environnement	ZoneCentral	ZC express
Moteur cryptographique opérant en mode kernel	☑	☑
Driver clavier « anti-keylogger »	☑	☑
Effacement par surcharge à la volée	☑	☑
Possibilité d'interdire la création de fichiers en clair sur les supports amovibles ou dans certaines zones	☑	☑
Administration		
Politique de sécurité sous forme de GPO (Group Polilicy Object), administrable en domaines	☑	☑
Installation automatisable (compatible SMS, Tivoli, etc.)	☑	☑
Délégation de droits de rôles, combinable avec les utilisateurs et groupes Windows	☑	
Mot de passe de secours	☑	☑
Administration « in-place », « back-office », ou distante	☑	
Outil d'administration graphique ou en ligne de commande(toutes opérations	☑	
Administration simplifiée, déléguée ou centralisée	☑	☑
Automate d'application, de réapplication ou de contrôle du plan de sécurité	☑	☑
Administration système, réseau et bureautique possible par un tiers « sans droit d'en connaître »	☑	☑

Pourquoi choisir ZoneCentral ?

- **Universalité**

  Un seul produit pour plusieurs cas d'applications : portables, supports amovibles (clé USB…), postes en réseau, serveurs de fichiers**…**

- **Facilité d'intégration dans le contexte de l'entreprise**

  Acceptabilité par les utilisateurs

  S'adapte à l'infrastructure de gestion de clés de l'entreprise

  Ne modifie pas l'exploitation du réseau

- **Evolutivité**

  Nouvelle technologie ouverte

- **Sécurité renforcée de l'environnement**

  Crypto implémentée sous forme de drivers

  Effacement par surcharge à la volée

  Etc.

- **Confiance : en cours de certification EAL2+ ; la cible concerne la totalité du produit , fonctions d'administration incluses**

Coordonnées

Siège :

10 place Béraudier
69428 Lyon Cedex 03
Tel : 04 26 68 70 02
Fax : 04 26 68 70 04

Direction commerciale :

42 avenue Montaigne
75008 Paris
Tel : 01 74 72 11 59
contact@primx.fr

Prim'X TECHNOLOGIES