



**Version 5.0**

# **Guide d'utilisation des conteneurs chiffrés**

**Révision 1**

---

# Reproduction et droits

Copyright © Prim'X Technologies 2003 - 2010

Toute reproduction, même partielle, du document est interdite sans autorisation écrite préalable de la société Prim'X Technologies ou de l'un de ses représentants légaux. Toute demande de publication, de quelque nature que ce soit, devra être accompagnée d'un exemplaire de la publication envisagée. Prim'X Technologies se réserve le droit de refuser toute proposition sans devoir justifier sa décision.

Tous droits réservés. L'utilisation du logiciel **Zed!** est soumise aux termes et conditions de l'accord de licence conclu avec l'utilisateur ou son représentant légal.

**Zed!** est une marque déposée de **Prim'X TECHNOLOGIES**.

# Sommaire

<b>Reproduction et droits</b> .....	<b>1</b>
<b>Sommaire</b> .....	<b>2</b>
<b>Evaluation Critères Communs</b> .....	<b>3</b>
<b>1. Introduction</b> .....	<b>5</b>
<b>2. Utilisation</b> .....	<b>6</b>
2.1. Première utilisation .....	6
2.1.1. Créer un nouveau conteneur .....	6
2.1.2. Lors de la toute première création d'un conteneur.....	6
2.2. Ouvrir un conteneur.....	9
2.2.1. Ouvrir un conteneur .....	9
2.3. Gérer le contenu d'un conteneur .....	11
2.3.1. Que peut contenir un conteneur ? .....	11
2.3.2. Lire un fichier du conteneur.....	11
2.3.3. Ouvrir un fichier du conteneur pour le modifier .....	11
2.3.4. Extraire des fichiers du conteneur .....	12
2.3.5. Renommer un fichier ou un dossier .....	13
2.3.6. Supprimer des fichiers ou des dossiers .....	13
2.3.7. Ajouter des fichiers .....	13
2.3.8. Créer un dossier .....	13
2.4. Depuis l'Explorateur Windows... .....	14
2.4.1. 'Envoyer vers'.....	14
2.4.2. L'icône du 'conteneur' est actif.....	14
2.5. Gérer les accès d'un conteneur.....	15
2.5.1. Rôles et accès spéciaux .....	15
2.5.2. Modifier les clés d'accès du conteneur.....	15
2.5.3. Retirer un accès.....	16
2.5.4. Changer un accès par mot de passe .....	16
2.5.5. Ajouter un accès par mot de passe.....	17
2.5.6. Utilisation du carnet de mot de passe .....	17
2.5.7. Ajouter accès par certificat RSA .....	18
2.5.8. Utilisation d'un annuaire de certificats .....	19
2.6. Options – Divers.....	19
2.6.1. Définir une image de marque .....	19
2.6.2. Panneau d'options.....	20
2.6.3. Changer de clé personnelle .....	20
<b>3. Messages d'erreur</b> .....	<b>22</b>
<b>4. Notes</b> .....	<b>24</b>

# Evaluation Critères Communs

Le produit **Zed!** v4.0 a été évalué conformément à la cible de sécurité version 1.10 de mai 2010 au niveau **EAL3+** (EAL3 augmenté des composants ALC\_FLR.3 et AVA\_VAN.3 associé à une expertise de l'implémentation de la cryptographie).

Afin d'utiliser le produit dans les conditions de l'évaluation, des mesures de sécurité portant sur l'environnement opérationnel doivent être suivies.

## Recommandations pour une utilisation dans les conditions de l'évaluation

**1/** L'environnement physique d'utilisation de la TOE doit permettre aux utilisateurs et aux administrateurs d'entrer leur mot de passe sans être observables directement ou sans que la saisie soit interceptable (clavier sans fil,...) par d'autres utilisateurs ou attaquants potentiels. Les mots de passe partagés entre les correspondants doivent être échangés à travers des canaux organisationnels protégés.

**2/** Lorsque l'utilisateur est authentifié, l'environnement opérationnel doit assurer la confidentialité des données sensibles et des données d'authentification.

Note d'application : L'équipement hôte doit apporter des protections efficaces contre l'écoute illicite et la transmission non autorisée de données (pare-feu correctement configuré, antivirus avec base de données à jour, « anti-spyware », etc.). Les applications installées sur l'équipement ne doivent pas perturber le bon fonctionnement du logiciel. Ainsi, les opérations que peut faire l'utilisateur sur les fichiers protégés par la TOE, surtout au travers de ses applications, ne doivent pas entraîner de copies totales ou partielles de ces fichiers en dehors de la TOE, sauf lorsqu'il l'a clairement demandé ou lorsque c'est une conséquence claire de l'opération demandée.

**3/** Les administrateurs de la TOE doivent être des personnes de confiance.

**4/** Les administrateurs Windows sont des personnes de confiance.

Les administrateurs de plus haut niveau du domaine Windows doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « polices » de la TOE. De même, les administrateurs de la TOE ne peuvent modifier les « polices ». En conséquence, ces administrateurs de plus haut niveau doivent eux-mêmes être des personnes de confiance.

Si les correspondants appartiennent à des entités gérés par des administrateurs de la sécurité de l'environnement Windows différents, ceux-ci doivent garantir ensemble l'utilisation de politiques de sécurité conformes au niveau recherché (force des mots de passe notamment). Dans le cas contraire, les échanges doivent s'effectuer avec un conteneur créé par chaque utilisateur et utilisé uniquement en émission.

**5/** Les utilisateurs de la TOE doivent être formés à l'utilisation de la TOE et sensibilisés à la sécurité informatique (ceci prend en compte la sensibilisation sur la qualité des clés d'accès et de leur support lorsqu'elles sont hébergées par un porte-clés). Les administrateurs de la TOE doivent recevoir une formation adaptée à cette fonction.

**6/** Les administrateurs de la TOE doivent être sensibilisés sur la qualité des clés d'accès qu'ils apportent à la TOE afin que ces clés soient conformes à l'état de l'art dans leur implémentation. Ils doivent également être sensibilisés à la qualité du support de ces clés lorsqu'elles sont hébergées par un porte-clés externe.

**7/** L'administrateur de la TOE est chargé de mettre en œuvre des procédures organisationnelles assurant la protection des certificats lors de leur remise aux utilisateurs. Il est également chargé, lors de la fourniture des clés d'accès possédant un certificat X509, vérifier la validité de ces certificats et leur adéquation avec l'usage qui en est fait par la TOE. Cette exigence s'applique en particulier aux certificats racines dits «authenticode» à partir desquels la vérification d'intégrité de la TOE peut être effectuée.

**8/** Les utilisateurs doivent conserver, dans un lieu sûr, les clés d'accès qui leur ont été transmises par un administrateur de la TOE et empêcher leur divulgation. L'administrateur de la TOE doit conserver ses clés de recouvrement dans un lieu sûr et empêcher leur divulgation.

**9/** Si les correspondants appartiennent à des entités gérées par des administrateurs de la sécurité de l'environnement Windows différents, ceux-ci doivent garantir ensemble l'utilisation de politiques de sécurité conformes au niveau recherché (force des mots de passe notamment). Dans le cas contraire, les échanges doivent s'effectuer avec un conteneur créé par chaque utilisateur et utilisé uniquement en émission.

**10/** En cas de coupure brutale de l'alimentation électrique alors que des conteneurs sont ouvertes, les effets de rémanence des mémoires physiques provoquent une persistance des données sensibles dans ces mémoires pouvant aller jusqu'à quelques dizaines de secondes. Si un tel événement se produit, l'utilisateur ne doit donc pas quitter son poste avant au moins une minute (à moins que la remise sous tension n'intervienne avant ce délai auquel cas les mémoires seront réinitialisées si l'utilisateur réamorce le système).

**11/** L'algorithme de chiffrement RSA est reconnu de niveau standard s'il est employé avec un module de taille supérieure ou égale à 1536 bits pour une utilisation n'allant pas au-delà de 2010 ou un module de taille supérieure ou égale à 2048 bits pour une utilisation n'allant pas au-delà de 2020, et si les exposants publics sont supérieurs à 65536.

**12/** Outre la recommandation ci-dessous, les clés RSA générées à l'extérieur du produit puis embarquées dans des fichiers de clés ou des objets physiques (pour être utilisées en tant que clés d'accès) doivent être générées conformément aux règles et recommandations de la DCSSI (Direction centrale de la sécurité des systèmes d'information).

**13/** L'algorithme RC2 n'est pas reconnu de niveau standard.

**Note :** Les administrateurs se répartissent selon 2 rôles :

- L'administrateur de la sécurité de l'environnement Windows des utilisateurs (administrateur Windows) en charge de définir les règles d'usage et de sécurité (les policies).
- L'administrateur de la TOE en charge de l'installation de la TOE, des opérations de recouvrement et de la mise à disposition des clés d'accès et éventuellement des mots de passe. Sauf mention contraire dans la suite de ce document, toute référence à l'administrateur se rapporte à ce rôle.

---

# 1. Introduction

**Zed!** est un produit très simple permettant de fabriquer des **conteneurs de fichiers chiffrés** (et compressés) destinés soit à être archivés soit à être échangés avec des correspondants, en pièces jointes de messages électroniques ou sur des supports variés, comme des clés mémoires USB.

L'utilisation des conteneurs chiffrés est très intuitive et tout à fait similaire à l'utilisation des 'dossiers compressés' sous Windows.

La version complète permet de définir les clés d'accès à un conteneur chiffré, soit sous forme de mots de passe "d'échange" convenus avec un correspondant, soit sous forme de certificats RSA, pris dans des fichiers certificats ou recherchés sur un annuaire LDAP de certificats. **Zed!** intègre par ailleurs une fonction très pratique, le '**Carnet de Mots de Passe**' qui permet de mémoriser et réutiliser les différents mots de passe des correspondants.

Il y a plusieurs usages possibles des conteneurs **Zed!**, un usage fréquent étant de préparer à l'avance et une fois pour toutes un conteneur pour chacun des quelques correspondants, avec les accès (clés) préparés, puis de réutiliser ce conteneur par la suite en changeant simplement les fichiers qu'il contient.

Ce document fait souvent référence aux politiques de sécurité décrites dans le **Manuel des politiques**.

## 2. Utilisation

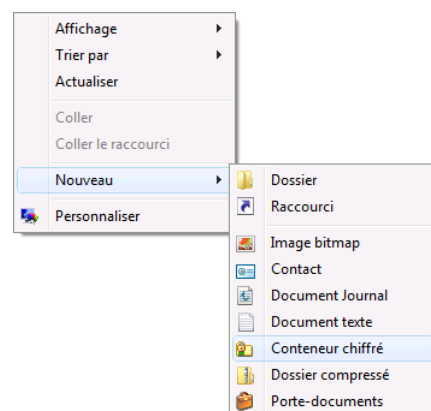
### 2.1. Première utilisation



#### 2.1.1. Créer un nouveau conteneur

Faites un click-droit dans le fond d'un dossier ou du bureau, déroulez le menu [Nouveau], et sélectionnez [Conteneur chiffré]. Un fichier est créé avec un nom par défaut, il vous est possible de changer son nom. Le conteneur est créé, mais n'est pas encore initialisé. Cela se fera automatiquement dès que vous l'ouvrirez.

L'extension des conteneurs chiffrés est ".zed".

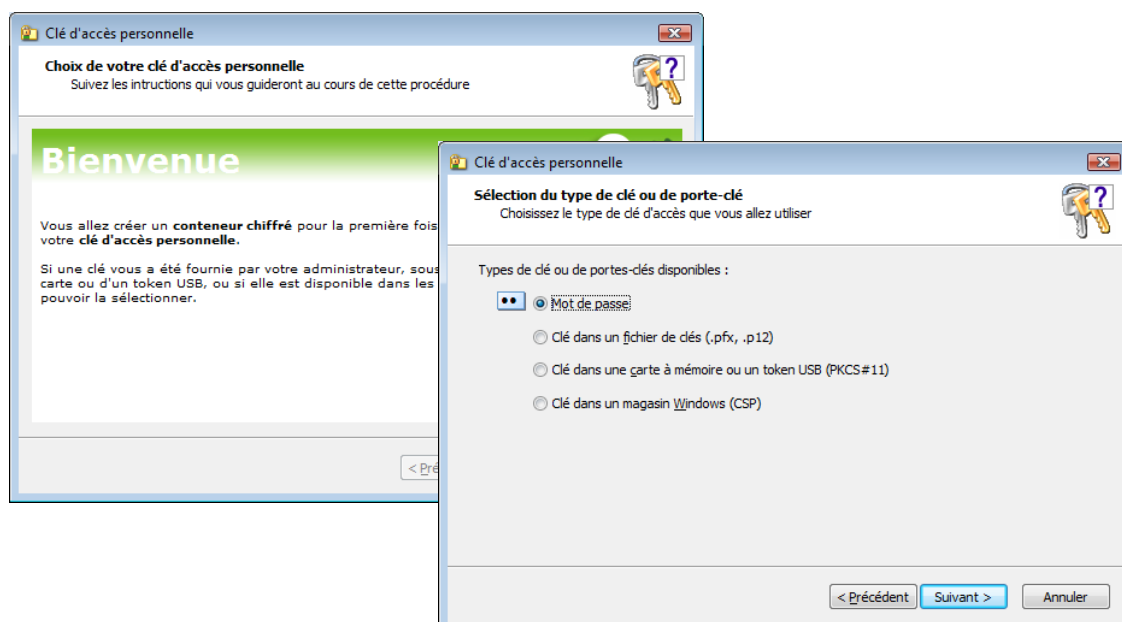


#### 2.1.2. Lors de la toute première création d'un conteneur

Dès que vous ouvrez le conteneur créé plus haut, un Assistant va apparaître pour vous faire choisir votre **clé d'accès personnelle**. Cette clé sera par la suite automatiquement intégrée dans chaque conteneur chiffré que vous créerez, ce qui vous permettra de les ouvrir par la suite.

Cet Assistant n'apparaît que la **première** fois. Ensuite, votre clé ayant été définie, il n'apparaîtra plus.

Cette clé sert également à protéger certaines informations liées à **zed !** sur votre ordinateur, notamment le Carnet de Mots de Passe, qui sera présenté plus loin.



Votre clé personnelle peut être :

- Un **mot de passe**, que vous choisissez ;
- Une **clé cryptographique RSA**, associée à un **certificat**, et qui peut être hébergée dans différents "porte-clés" :
  - Un fichier de clés (.pfx ou .p12, en général), protégé par mot de passe ;
  - Une carte à puce ou un token USB, de type RSA (la plupart des fabricants du marché sont supportés), respectant la norme PKCS#11 ;
  - Un conteneur de clés CSP de Windows, ce conteneur pouvant être dans les magasins de votre profil utilisateur Windows ou dans un magasin "tierce-partie" (parmi lesquels on peut retrouver aussi les cartes à puce ou tokens USB RSA)

**Note** : le logiciel **Zed!** ne génère pas de clés RSA ni de certificats. Si vous souhaitez utiliser des clés de ce type, vous devez utiliser les services d'une PKI (infrastructure de certificats) d'entreprise, ou publique, ou commerciale.

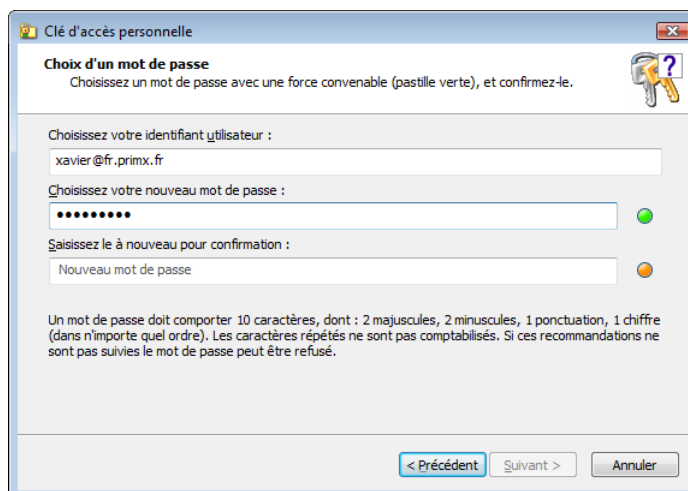
**Variantes** : votre administrateur Windows a pu configurer les politiques de sécurité du produit pour modifier le comportement de cette étape :

- Il peut retirer certaines possibilités (interdire les mots de passe, par exemple) ;
- Il peut imposer une force minimale aux mots de passe ;
- Dans le cas de clés RSA, il peut imposer certaines règles sur les certificats et clés utilisables ;
- Il a également pu faire en sorte d'imposer des jeux de clés RSA prédéfinis au sein du domaine Windows et publiés sur le contrôleur de votre domaine : vous n'aurez pas le choix de la clé à utiliser, il vous faudra fournir celle qui vous a été imposée (et remise par ailleurs, ou que vous utilisez déjà depuis longtemps pour d'autres usages).

## **Choix d'un mot de passe**

Dans la page suivante, vous devez choisir un **identifiant d'utilisateur**. Par défaut, le produit vous propose votre nom d'utilisateur Windows, mais vous pouvez le changer. Ce nom sera utile par la suite pour "vous reconnaître" dans les différents accès prévus dans un conteneur. Quand vous le verrez apparaître, vous saurez que c'est votre mot de passe qu'il faut fournir.

→ une bonne pratique, également, est de mettre son adresse email.



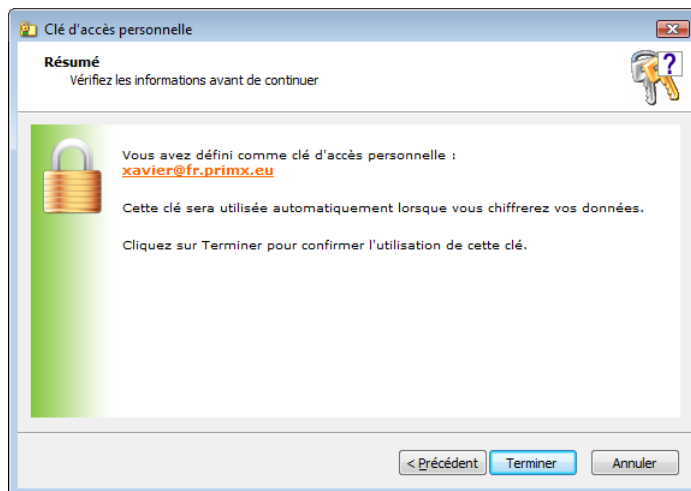
Il vous faut ensuite vous choisir un **mot de passe personnel**, que vous devrez fournir deux fois, pour bien vous assurer de le connaître. Dans la première saisie, la pastille reste rouge tant que votre mot de passe n'a pas une "force" suffisante. Dans la seconde saisie, la pastille est orange tant que vous ne faites pas d'erreur, devient verte dès que la saisie est la même que la première, et rouge si vous faites une erreur.



Pour augmenter la "force" de votre mot de passe, une bonne pratique est de faire varier les caractères : minuscules, majuscules, chiffres, caractères de ponctuation. En rendant ainsi plus "large" l'espace des valeurs possibles pour un même caractère, vous augmentez la force. Sinon, vous devez compenser par la longueur du mot de passe. C'est une question d'équilibre entre "mot de passe court mais complexe" et "mot de passe long mais simple".

**Note** : votre administrateur Windows a pu imposer le niveau de force. Par défaut, la configuration vous oblige à mettre un mot de passe de force raisonnable, un peu au dessus de la moyenne.

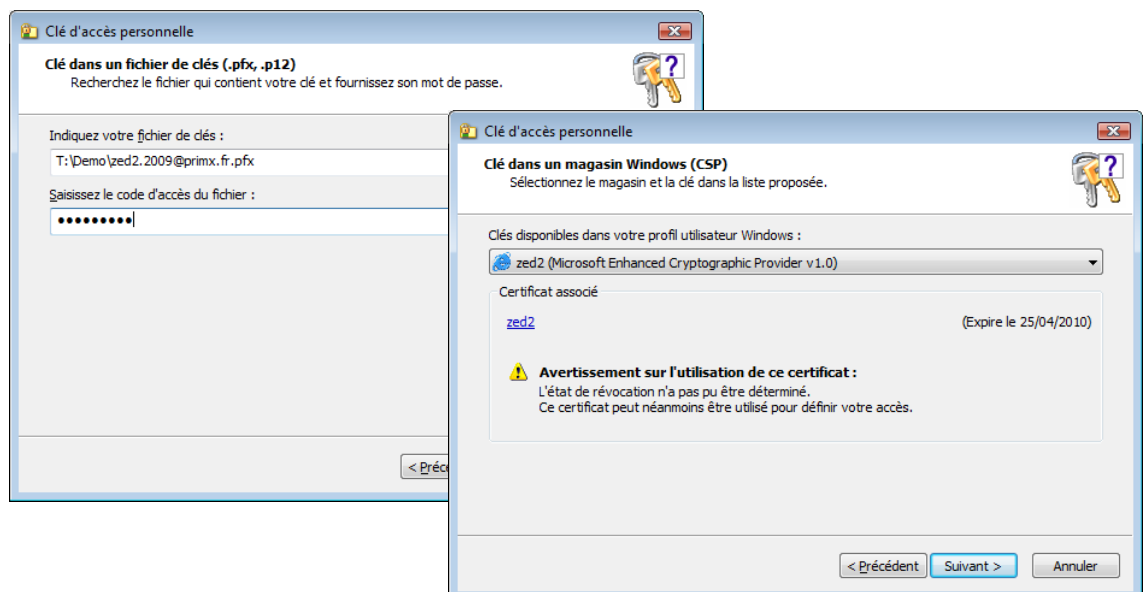
Validez, et l'opération est terminée. Elle ne sera plus à faire ensuite.



### Choix d'un certificat

L'opération pour un certificat et une clé RSA est très similaire : vous êtes invité, en fonction des cas, à choisir un fichier de clés, ou introduire votre carte ou token USB, ou encore à choisir votre certificat.

Vous devrez fournir le code d'accès (du fichier, de la carte, ...), et valider. S'il y a plusieurs clés disponibles, le produit les étudie, élimine celles qui ne sont pas utilisables dans son contexte, et vous laisse le choix.



## 2.2. Ouvrir un conteneur



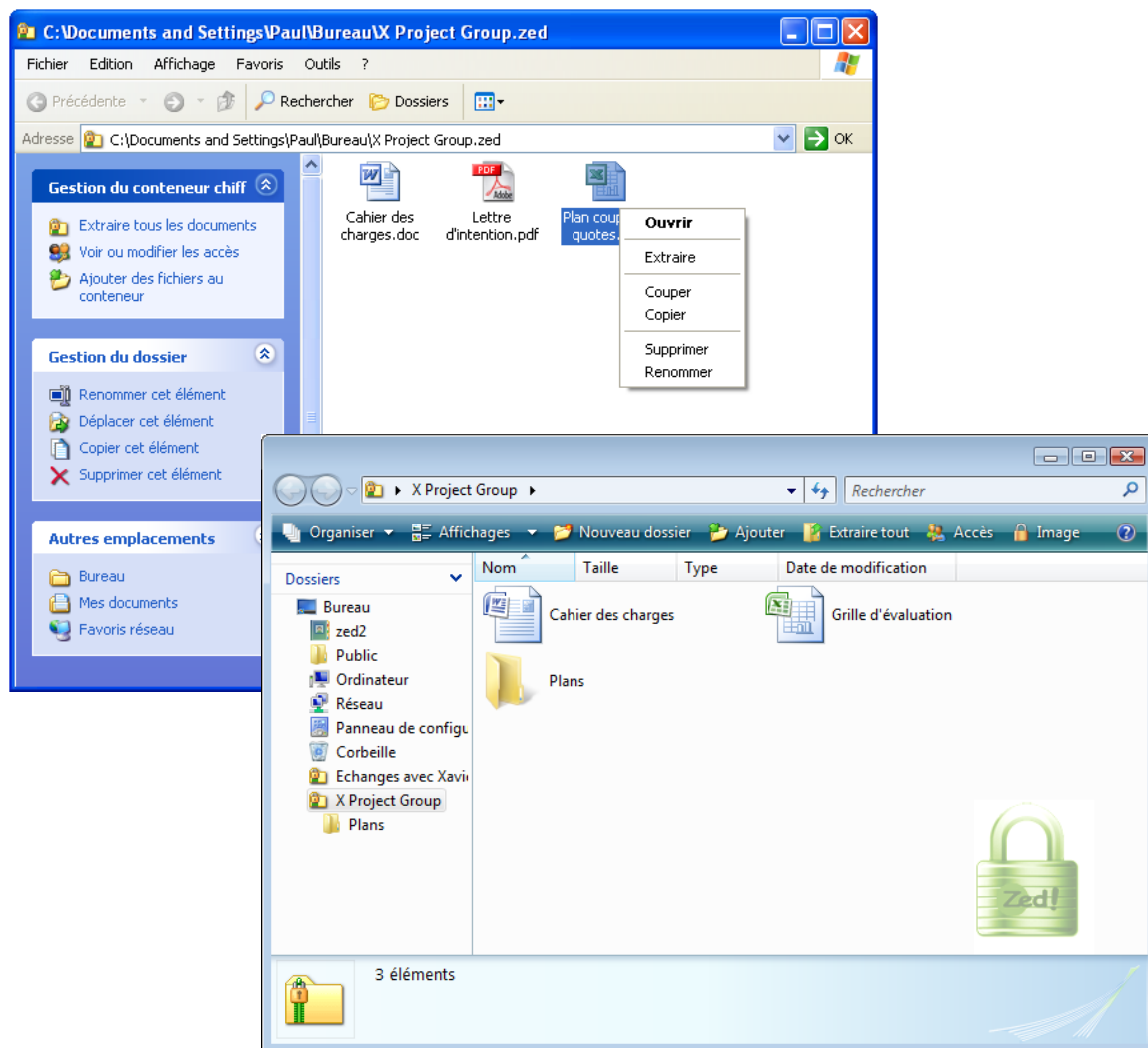
### 2.2.1. Ouvrir un conteneur

Il suffit de double-cliquer dessus ou d'utiliser le menu contextuel [ouvrir]. Le conteneur s'affiche, avec les fichiers qu'il contient.

V5.0

Si la clé d'accès n'a pas été encore fournie, les noms des fichiers affichés sont masqués : ils ont une forme générique, par exemple « File1.doc » ou « Folder1 ». Les véritables noms de fichiers ne sont visibles que lorsque le conteneur est ouvert au sens cryptographique (on a saisi la clé d'accès). Cette ouverture cryptographique est effectuée lorsqu'on ouvre un fichier du conteneur, ou lorsqu'on choisit dans le menu l'action « Ouvrir le conteneur ».

Voici un aperçu sous Windows XP et Windows Vista :

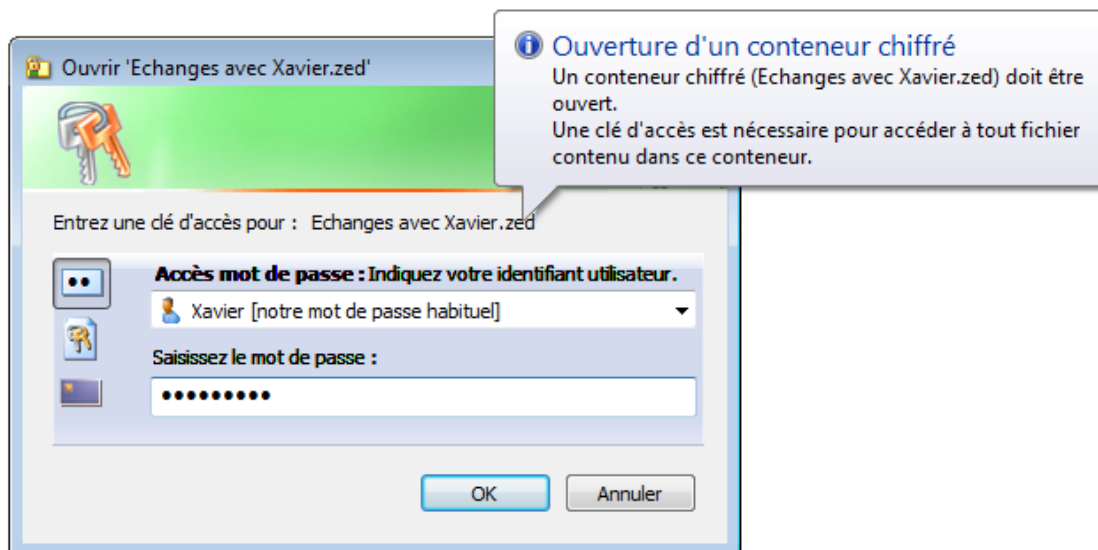


Le style et l'ergonomie de ce 'pseudo-dossier' sont très similaires à ceux des dossiers compressés (.zip) natifs sous Windows. Toutes les opérations habituelles sur les fichiers sont autorisées (glisser-déplacer, copier-coller, changement de nom, suppression, etc.). Cependant, dès qu'une de ces opérations entraîne le chiffrement ou le déchiffrement d'un fichier, la clé d'accès va être demandée (voir plus loin).



## 2.2.2. Donner la clé d'accès au conteneur

A la première opération sur un fichier du conteneur, une clé d'accès va être demandée. Il peut s'agir d'un mot de passe convenu avec la personne qui vous a expédié ce conteneur (ici, 'Xavier'), ou d'une clé RSA, que vous détenez dans un fichier de clés (.pfx), une carte à mémoire, ou qui est hébergée dans un magasin de clé de Windows (CSP).



Sélectionnez le pictogramme correspond au type de clé d'accès que vous possédez. Le premier désigne des mots de passe, le second des fichiers de clés (.pfx), et le troisième une carte à mémoire. Pour ces deux derniers, il vous faudra saisir le code confidentiel associé.

La clé d'accès fournie est ensuite conservée en mémoire un certain temps.

Le cas échéant, elle sera redemandée lors d'une autre opération si besoin est.

### Notes :

Si votre clé d'accès est hébergée dans un magasin de clés Windows (CSP), et si elle peut effectivement ouvrir le conteneur, alors cette fenêtre n'apparaît pas. Soit l'ouverture est automatique, sans demande, soit c'est la fenêtre du CSP utilisé qui sera affichée (cela dépend des dispositifs CSP additionnels éventuels installés sur votre poste) ;

Le logiciel **Zed!** est prévu pour reconnaître en standard un certain nombre de cartes à mémoire RSA (ou tokens USB). Si votre carte n'apparaît pas dans la liste, c'est certainement qu'elle n'est pas d'un type préconfiguré. Dans ce cas, il est possible de contacter le support technique qui vous indiquera la procédure technique pour configurer votre type de carte (si elle est compatible).

## 2.3. Gérer le contenu d'un conteneur



### 2.3.1. Que peut contenir un conteneur ?

Un conteneur peut être considéré comme un dossier 'habituel' : il peut contenir autant de fichiers qu'on le souhaite, de toutes natures (il n'y a aucune restriction), classés en dossiers et sous-dossiers éventuellement.

On retrouvera également la plupart des opérations classiques des dossiers 'Windows' : copier un ou plusieurs fichiers/dossiers, les déplacer ou les coller ailleurs (à l'intérieur du conteneur ou à l'extérieur), renommer des fichiers ou des dossiers, en supprimer, etc.

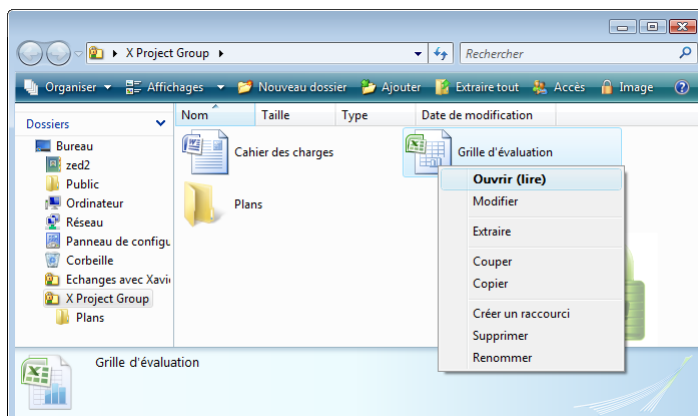
Un conteneur se traite donc de façon très similaire à un dossier classique, la différence étant qu'il est « transportable » (in fine, c'est un fichier qui en contient d'autres), et que son contenu est à la fois compressé et crypté (et donc qu'il faut disposer d'une clé d'accès pour y accéder).



### 2.3.2. Lire un fichier du conteneur

Cette opération demande une clé d'accès si elle n'a pas déjà été fournie précédemment.

Il suffit de sélectionner le fichier et de double-cliquer dessus, ou bien d'afficher le menu contextuel (click droit) et de faire le choix [ouvrir (lire)]. Le fichier est extrait, déchiffré et décompressé, et copié dans un fichier temporaire, puis l'application qui traite habituellement ce type de fichier sur votre poste est activée et l'ouvre.



Si un fichier du même nom existe déjà dans l'emplacement temporaire, il vous sera demandé si vous souhaitez le remplacer ou non.

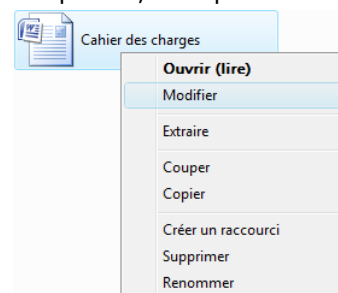
ATTENTION, il s'agit ici d'une LECTURE. Le fichier est donc ouvert en lecture seulement, et l'application lancée **ne pourra pas le modifier**.



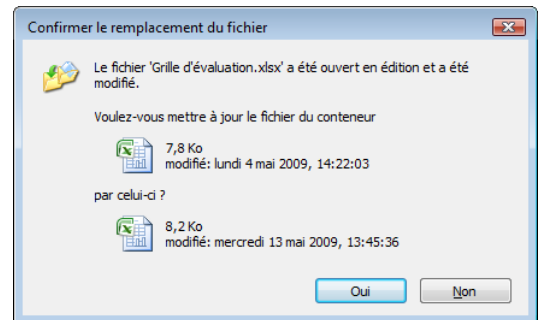
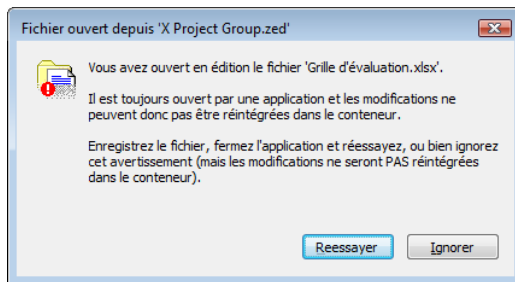
### 2.3.3. Ouvrir un fichier du conteneur pour le modifier

Il faut utiliser le choix [modifier]. Le fichier est extrait, déchiffré et décompressé, et copié dans un fichier temporaire, puis l'application qui traite habituellement ce type de fichier sur votre poste est activée et l'ouvre. Contrairement au cas précédent, le fichier est accessible en écriture et peut être modifié avec l'application lancée.

Comme le fichier a été extrait dans un fichier temporaire dans un endroit 'technique' de votre environnement de travail, il n'est pas aisé d'aller le récupérer après modification pour le remettre dans le conteneur après modification. Ce n'est pas grave, **le logiciel fera cela pour vous automatiquement**.



Dès que vous fermerez le conteneur ou que vous changerez de dossier avec la fenêtre qui affiche le conteneur, alors automatiquement les fichiers qui ont été extraits pour modification, et qui ont effectivement été modifiés, seront réintégrés. Pour ne pas risquer cependant de faire d'erreur, la question vous est posée (voir ci-contre).



Si le fichier en question est toujours ouvert et verrouillé par l'application, il est impossible de réintégrer son contenu. Là encore, vous êtes prévenu, ce qui vous laisse éventuellement la possibilité de retourner dans l'application, de sauvegarder votre travail, et de fermer le fichier.

**Nettoyage** : il n'est pas inutile de savoir que tous ces fichiers ouverts dans un dossier temporaire (pour lecture ou pour modification) sont nettoyés automatiquement (avec effacement du contenu) quand le conteneur est fermé ou quand vous changez de dossier. Le seul cas où le nettoyage n'est pas effectué est le cas où un fichier est toujours verrouillé par l'application. Dans ce cas, vous êtes également prévenu : il est recommandé de fermer l'application, puis d'utiliser le bouton [Réessayer] afin de procéder au nettoyage et ainsi de laisser le moins de résidus de données possibles 'hors conteneur'.

#### Remarques :

- Le dossier temporaire dans lequel sont automatiquement extraits les fichiers pour lecture ou modification peut être configuré dans les [options]. Il est ainsi possible de choisir le Bureau, ce qui rend plus accessibles les fichiers.
- L'action par défaut du [double-click] sur un fichier peut également être configurée dans les [options], ce qui permet de choisir entre [ouvrir (lire)] et [modifier].



### 2.3.4. Extraire des fichiers du conteneur

Cette opération demande une clé d'accès si elle n'a pas déjà été fournie précédemment.

L'extraction consiste à déchiffrer, décompresser et déposer à un emplacement désigné le ou les fichiers sélectionnés.

Il y a plusieurs façons d'effectuer cette opération :

- Faire un [copier] des fichiers dans le conteneur, suivi d'un [coller] à l'emplacement où vous voulez que les fichiers soient déposés (sur le bureau, dans un autre dossier, etc. (les accélérateurs clavier [Ctrl-C/Ctrl-V] fonctionnent également, de même que le [couper/coller]) ;
- Faire un [glisser/déplacer] à la souris des fichiers sélectionnés dans le conteneur vers l'emplacement où vous voulez que les fichiers soient déposés ;
- Utiliser le menu contextuel [Extraire] sur les fichiers du conteneur : dans ce cas, une fenêtre apparaît pour que vous puissiez sélectionner l'emplacement cible ;
- Utiliser le menu contextuel [Extraire tout] dans le 'fond' du conteneur : dans ce cas, une fenêtre apparaît pour que vous puissiez sélectionner l'emplacement cible, et TOUS les fichiers seront alors extraits.

S'il existe déjà un ou plusieurs fichiers de même nom dans l'emplacement cible, une fenêtre vous demandera confirmation du remplacement.



### 2.3.5. Renommer un fichier ou un dossier

Cette opération est possible et ne demande pas de clé d'accès. Utiliser la touche standard [F2] ou encore le menu contextuel [Renommer] et indiquer le nouveau nom (qui doit respecter les contraintes habituelles sur les noms de fichiers).



### 2.3.6. Supprimer des fichiers ou des dossiers

Cette opération demande une clé d'accès. Utiliser la touche [Suppr] ou le menu contextuel [Supprimer] sur les éléments sélectionnés.

Si c'est un dossier qui est supprimé, tous les fichiers (et dossiers) qu'il contient sont également supprimés.

Attention, il n'y a **pas de mise en "Corbeille"** des fichiers supprimés dans un conteneur.



### 2.3.7. Ajouter des fichiers

Cette opération demande une clé d'accès si elle n'a pas déjà été fournie précédemment.

L'ajout consiste à copier le fichier source, compresser son contenu, et à le chiffrer dans le conteneur.

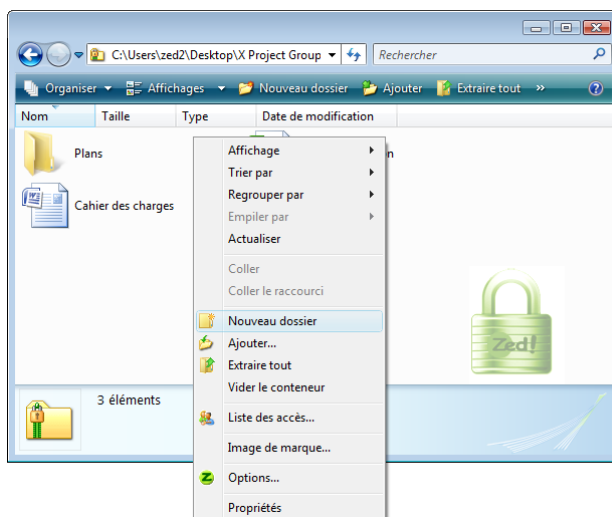
Il y a plusieurs façons d'effectuer cette opération :

- Faire un [copier] des fichiers 'source', suivi d'un [coller] dans le conteneur (les accélérateurs clavier [Ctrl-C/Ctrl-V] fonctionnent également, de même que le [couper/coller]) ;
- Faire un [glisser/déplacer] des fichiers 'source' vers le conteneur ;
- Utiliser le menu contextuel [Ajouter...] dans le 'fond' du conteneur : dans ce cas, une fenêtre apparaît pour que vous puissiez sélectionner les fichiers 'source'.



### 2.3.8. Créer un dossier

Cette opération demande une clé d'accès. Utiliser le menu contextuel [Nouveau dossier] dans le 'fond' du conteneur :

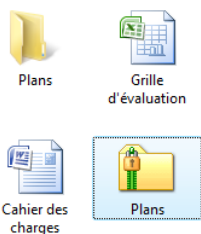
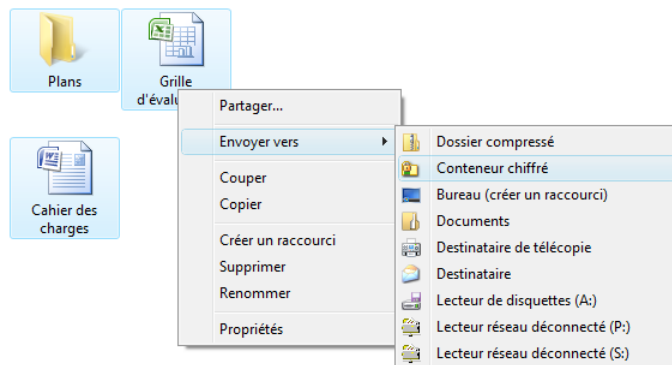


## 2.4. Depuis l'Explorateur Windows...



### 2.4.1. 'Envoyer vers'

A partir de la sélection d'un ou plusieurs fichiers ou dossiers, il est possible d'utiliser le menu [Envoyer vers] de Windows pour lequel une option [Conteneur chiffré] a été ajoutée.

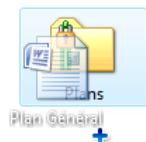


Un nouveau conteneur est alors créé (avec comme unique accès votre clé personnelle) et les fichiers et dossiers sélectionnés dans l'Explorateur (ou le Bureau) sont ajoutés (copiés) dans le conteneur.

Le nouveau conteneur prend comme nom celui du premier élément de la sélection.

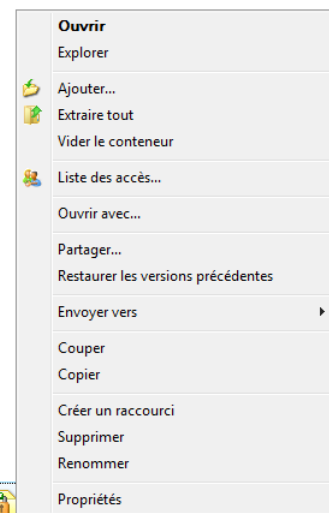


### 2.4.2. L'icône du 'conteneur' est actif



Il est possible de glisser/déplacer des fichiers et ou dossiers directement au dessus de l'icône du conteneur, sans l'ouvrir, pour ajouter ces fichiers au conteneur

De même, le fichier conteneur présente un certain nombre de choix spécifiques dans son menu contextuel, ce qui permet d'effectuer certaines opérations sans l'ouvrir véritablement.



## 2.5. Gérer les accès d'un conteneur

V5.0

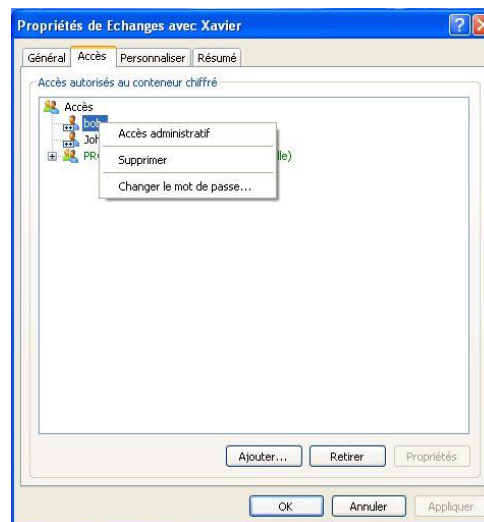


### 2.5.1. Rôles et accès spéciaux

A chaque accès est associé un **rôle** :

- "administratif" : quand un utilisateur a le droit non seulement d'accéder aux fichiers du conteneur, mais a en plus le droit de procéder à des opérations de gestion sur les accès. Le créateur d'un conteneur a toujours ce rôle ;
- "normal" : quand un utilisateur n'a pas d'autre rôle que d'accéder aux conteneurs et utiliser les fichiers qu'ils contiennent. C'est le rôle qui est attribué par défaut aux nouveaux accès ajoutés ;
- "recouvrement" : configurable par politique. Ce type d'accès ne doit normalement pas servir en utilisation courante.

Des options de menu permettent à un utilisateur possédant le rôle administratif d'affecter ou de retirer le rôle administratif aux autres utilisateurs.



### 2.5.2. Modifier les clés d'accès du conteneur



Cette opération nécessite un rôle **administratif**.

Lorsqu'il est créé, un conteneur contient toujours votre accès personnel, avec **vosre clé personnelle**.

Remarque : si le conteneur a été créé par quelqu'un d'autre, et qu'il vous a été envoyé, il ne contiendra pas forcément votre clé personnelle. Si vous avez une clé RSA, ce sera généralement le cas puisque votre correspondant aura utilisé votre certificat. Mais s'il s'agit d'un mot de passe, il est plus probable qu'il s'agira d'un mot de passe convenu entre vous, qui ne sera pas forcément le même que votre mot de passe habituel (sauf si vous avez convenu de celui-là).

Le conteneur peut aussi contenir d'autres accès, de type **RSA**, qui sont **imposés par votre administrateur Windows** dans la configuration du produit.

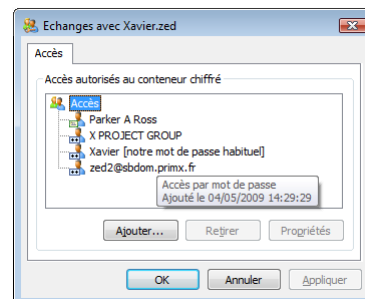
Si vous souhaitez qu'un conteneur serve de "**valise diplomatique**" d'échange avec une ou plusieurs personnes, vous devez d'abord convenir d'un "secret" avec eux. Si votre correspondant dispose d'une clé RSA et du certificat associé, vous pouvez utiliser directement ce certificat. Sinon, vous pouvez convenir avec lui d'un mot de passe.



→ Pour accéder à la gestion des accès, vous pouvez au choix :

- Utiliser le menu contextuel sur le fichier conteneur lui-même (click-droit sur le fichier, option [Liste des accès] ;
- Ouvrir le conteneur, et faire un click-droit dans le fond de la fenêtre, option [Liste des accès].

La fenêtre qui apparaît présente les accès existants, et permet d'en ajouter ou d'en retirer. Quand il s'agit d'accès par clé RSA/Certificat, vous pouvez consulter le certificat.



Noter le pictogramme qui diffère en fonction du type d'accès, et la bulle d'aide qui donne des informations complémentaires.



### 2.5.3. Retirer un accès

Cette opération nécessite un rôle **administratif**.

A partir de la fenêtre précédente, il suffit de sélectionner l'accès et d'utiliser le bouton [Retirer] ou le menu contextuel [Supprimer]. Après confirmation, l'accès est retiré de la fenêtre.

Lorsque toutes les modifications sur les accès sont terminées, vous pouvez utiliser le bouton [Appliquer] pour les rendre opérationnelles, ou encore le bouton [OK] (qui, lui, fermera aussi la fenêtre).

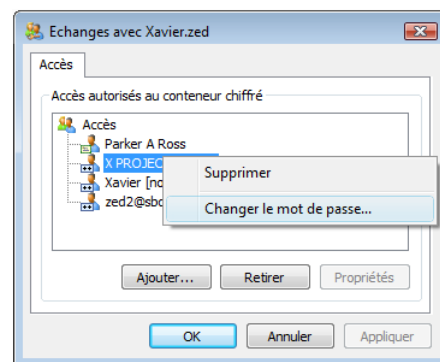
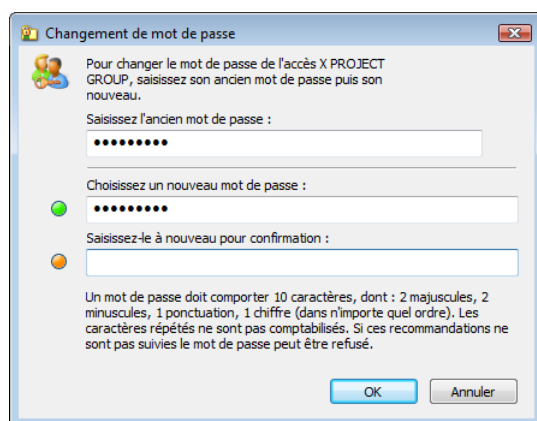
Noter que dès que les accès sont modifiés, mais pas enregistrés, le titre de la liste ("Accès") prend un astérisque ("Accès\*").

Les accès imposés par votre administrateur Windows ne peuvent pas être retirés.



### 2.5.4. Changer un accès par mot de passe

Toujours à partir de la fenêtre des accès, sélectionner un accès de type mot de passe utiliser le menu contextuel [Changer le mot de passe].



Comme pour toute création de mot de passe, il doit être saisi deux fois pour vérification, et obéir aux contraintes de "force" qui sont affichées.



## 2.5.5. Ajouter un accès par mot de passe

Cette opération nécessite un rôle **administratif**.

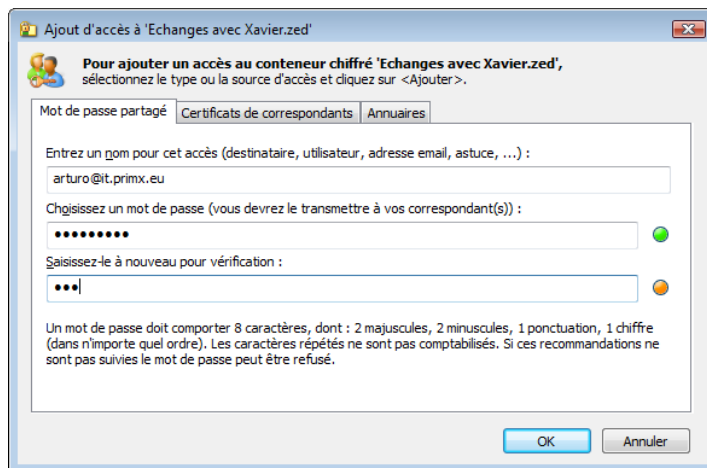
A partir de la fenêtre des accès, cliquer sur le bouton [Ajouter]. Une fenêtre apparaît avec plusieurs onglets, dont notamment le premier s'appelle [Mot de passe partagé]. Sélectionnez-le, puis :

- Choisissez un nom pour cet accès. Ce nom peut dépendre de la façon dont il va être utilisé. S'il s'agit simplement d'une convention privée avec un autre personne, vous pouvez entrer son adresse email, par exemple. S'il s'agit d'un accès qui sera utilisé par plusieurs personnes, vous pouvez mettre le nom d'un groupe de travail.

Cette information est libre, mais doit être claire, parce qu'elle apparaît ensuite dans la demande de clé quand on accède au contenu du conteneur.

- Tapez le mot de passe convenu, ou choisissez-en un nouveau, que vous transmettez ensuite au(x) correspondant(s), par un canal secondaire.

Comme pour toute création de mot de passe, il doit être saisi deux fois pour vérification, et obéir aux contraintes de "force".



V5.0

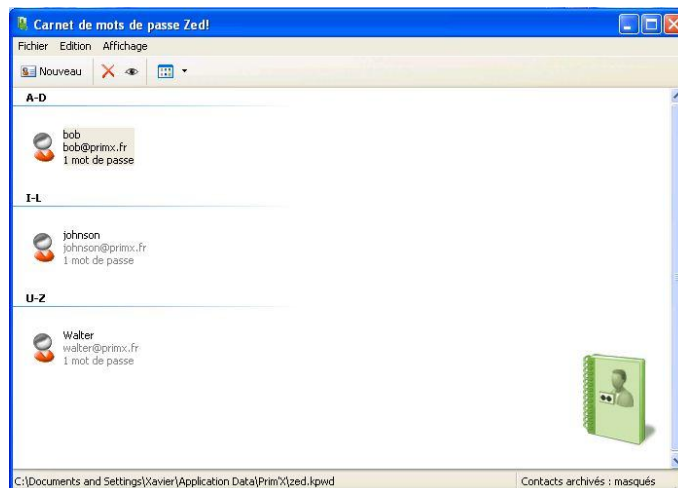


## 2.5.6. Utilisation du carnet de mot de passe

Votre Carnet de Mots de Passe est personnel.

Le carnet de mot de passe contient l'enregistrement de tous les mots de passe que vous avez définis pour vos correspondants :

- Soit en ajoutant un mot de passe pour un destinataire, qui n'avait pas encore de clé, et vous avez choisi un mot de passe ou demandé à **Zed!** d'en générer un pour vous ;
- Soit en recevant un conteneur d'un destinataire pour la première fois : pour le lire, vous avez dû taper le mot de passe qu'il vous a donné, et il est automatiquement enregistré dans le Carnet.

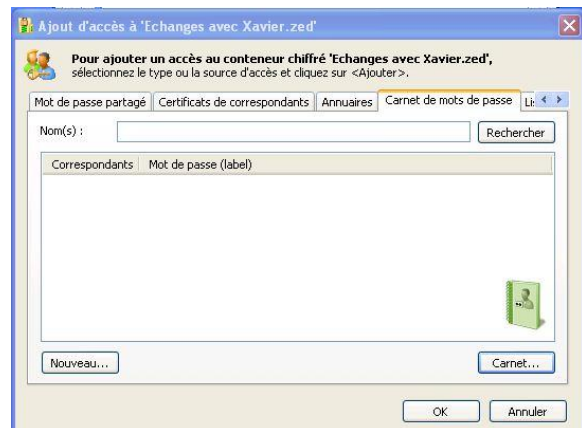


Le Carnet de Mot de Passe est bien entendu protégé et chiffré, avec votre Clé Personnelle.

**Il ne faut surtout pas confondre votre Mot de Passe Personnel avec les Mots de Passe d'Echange !**

Vous n'avez un Mot de Passe Personnel que si c'est la solution que vous avez retenue pour vous-même lors du choix de votre Clé Personnelle. Cela aurait très bien pu être un Certificat, ce qui ne vous empêcherait pas par ailleurs d'échanger avec des correspondants 'à mots de passe'.

A partir de la fenêtre des accès, cliquer sur le bouton [Carnet de mots de passe] pour accéder à la fenêtre de gestion du carnet (le carnet peut également être affiché à partir de l'onglet des options décrit plus loin).



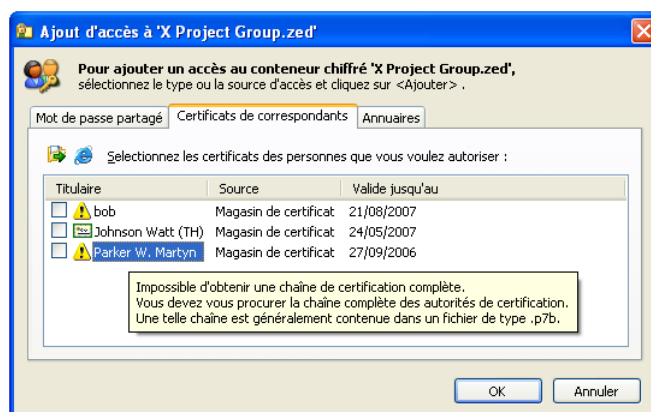
### 2.5.7. Ajouter accès par certificat RSA

Cette opération nécessite un rôle **administratif**.

A partir de la même fenêtre, sélectionner l'onglet [Certificats de correspondants] ou l'onglet [Annuaire]. L'utilisation des annuaires est décrite au paragraphe suivant.

Localement, sur votre ordinateur, les certificats peuvent être trouvés dans :

- Des fichiers de certificats. Il y a de multiples formats standards, la plupart sont supportés (fichiers avec les extensions .cer, .p7b, etc.). Si vos correspondants vous donnent leurs certificats sous forme de fichiers, vous les déposez habituellement dans un dossier, et vous pouvez ici rechercher ces fichiers, en sélectionner plusieurs, et vous pourrez voir les certificats qu'ils contiennent, et sélectionner ceux qui vous intéressent.
- Des magasins de certificats que gère votre système Windows, ce qui est une autre manière de les enregistrer quelque part pour pouvoir les retrouver. Vous pouvez les gérer avec l'Internet Explorer, menu [Outils], onglet [Contenu], bouton [Certificats]. C'est pourquoi, en appuyant sur le bouton qui reprend le pictogramme de Internet Explorer, la fenêtre se remplit avec les certificats disponibles dans ces magasins.



Les certificats sont vérifiés en temps réel dans cette fenêtre. En fonction des résultats, ils ont un pictogramme qui diffère.

Le pictogramme "sablier" indique que la vérification est en cours. Elle peut parfois prendre un peu de temps, s'il faut télécharger des listes de révocation (CRLs).

→ Penser à faire afficher la bulle d'aide pour connaître la raison d'un statut de vérification.  
 → Noter également l'existence de menus contextuels, sur les certificats et dans le fond de la liste, qui permettent :

- d'afficher un certificat ;
- de refaire une vérification sur un certificat ;
- de tout décocher, tout cocher, et demander à ce que les certificats soient cochés ou décochés par défaut quand ils sont affichés (s'ils sont utilisables).

Lorsque l'échec du contrôle est dû à des raisons 'externes' (état de révocation par exemple), le certificat apparaît avec un pictogramme d'avertissement, et son utilisation est tolérée. En effet, les conteneurs sont un outil d'échange, et il est souvent difficile d'effectuer une vérification complète avec des certificats en provenance de sociétés tierces.



### 2.5.8. Utilisation d'un annuaire de certificats

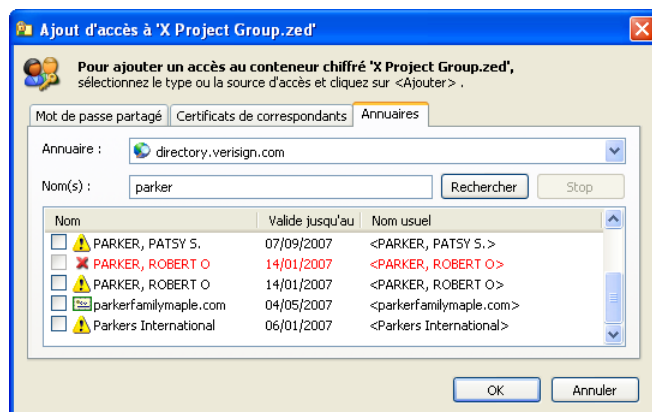
Certaines entreprises mettent à disposition des annuaires (appelés "annuaires LDAP") permettant de retrouver les certificats des personnes, à partir de leur nom ou d'une adresse email. C'est souvent le cas également d'organismes de certification publics ou commerciaux.

La recherche s'effectue en donnant l'adresse de l'annuaire, et le nom, partiel ou complet, à rechercher. Elle demande évidemment une connexion disponible vers l'annuaire ciblé.

Si votre ordinateur fait partie d'un domaine Windows, qui, souvent, intègre un annuaire LDAP, son adresse est détectée et proposée. Cela fonctionne si, en interne, il y a une PKI (infrastructure de certificats) et que les certificats sont publiés à cet endroit.

Un exemple de serveur disponible librement est "directory.verisign.com", vous pouvez essayer avec des noms américains, comme "parker" ou "johnson".

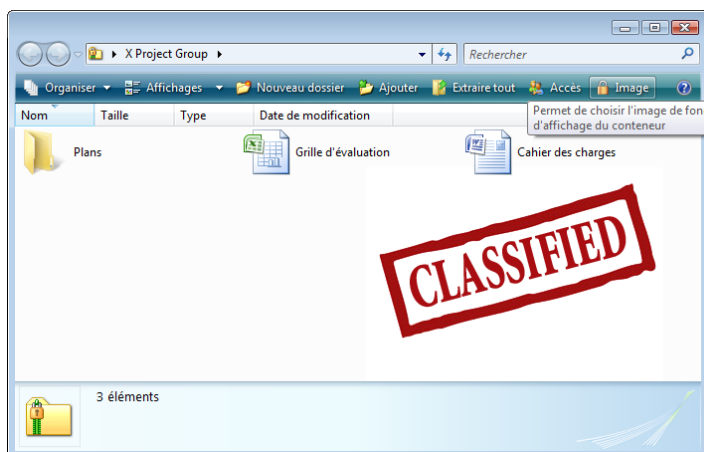
Dans cette fenêtre, on retrouve les mêmes options dans les menus contextuels que pour la précédente.



## 2.6. Options – Divers

### 2.6.1. Définir une image de marque

Par défaut, les conteneurs ont une image de 'fond' par défaut (un cadenas vert). Il est possible de définir soi-même l'image de fond d'un conteneur donné, et de faire en sorte que cette image soit « embarquée » dans le conteneur : elle est ainsi transportée avec lui, et un autre lecteur verra donc ce conteneur avec cette image.



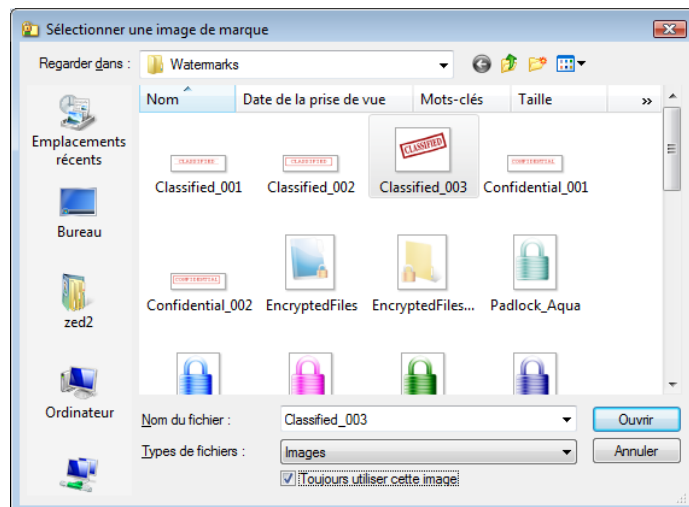
⚠ Les images de marque ne sont affichées que si les couleurs des listes sous Windows sont blanches ou très proches du blanc. Sinon, elles ne sont pas affichées.

Le choix de l'image s'effectue à partir de la barre d'outils (comme ci-dessus) ou à partir du menu contextuel (click-droit) dans le 'fond' du conteneur ou sur le fichier conteneur lui-même.

Vous pouvez sélectionner une des images livrées avec le logiciel, ou choisir une image qui vous est propre, pour un marquage personnalisé 'Société' par exemple.

Noter tout en bas la case à cocher [Toujours utiliser cette image] : si vous ne la cochez pas, l'image choisie s'appliquera seulement au conteneur courant. Si vous la cochez, tous vos conteneurs nouvellement créés utiliseront cette image.

Remarque : pour annuler ce choix ultérieurement, il faudra revenir dans cette fenêtre, cocher la case, et [Annuler].



### 2.6.2. Panneau d'options

Le panneau d'options est accessible à partir du menu contextuel (click-droit) dans le 'fond' du conteneur ou sur le fichier conteneur lui-même.

Le panneau d'options permet de configurer certaines options de fonctionnement et de consulter la version du logiciel.

La première option concerne l'action à prendre quand un [double-click] est effectué sur un fichier : soit ouvrir le fichier en lecture seule (cf.§2.3.2), soit ouvrir le fichier pour le modifier (cf.§2.3.3).

La seconde option permet de définir l'emplacement dans lequel sont automatiquement extraits et copiés les fichiers qui sont ouverts pour lecture ou pour modification (cf.§2.3.2). Le cas [automatique] définit cet emplacement dans un dossier technique de votre profil utilisateur Windows (là où sont habituellement déposés les fichiers temporaires).



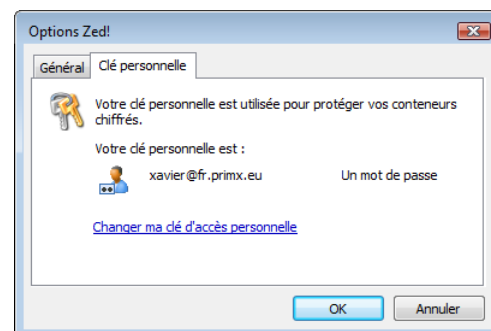
**V5.0**

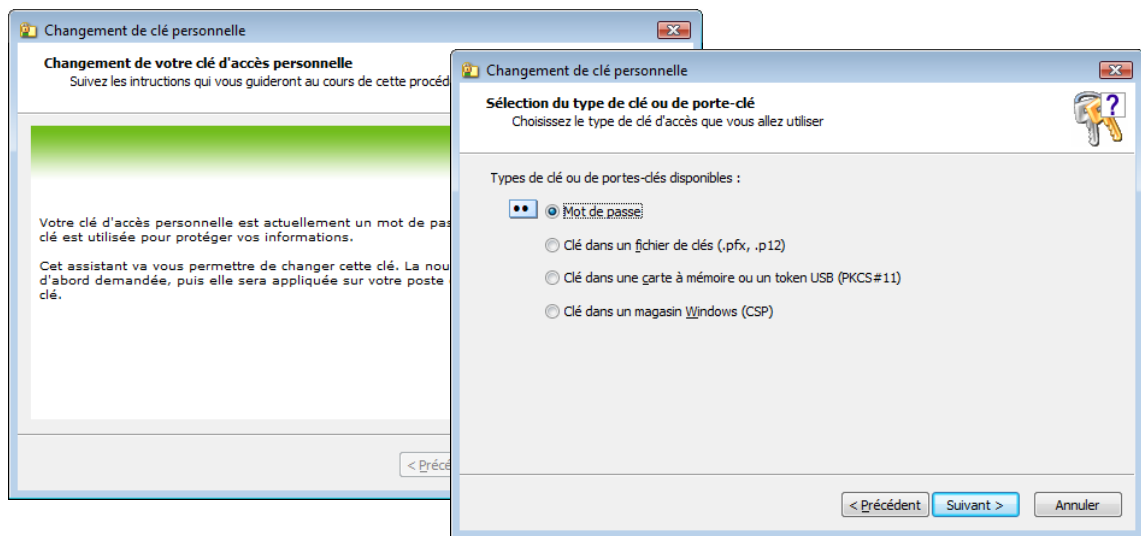
Le carnet de mot de passe (cf.§2.5.6) peut également être affiché à partir de ce panneau.

### 2.6.3. Changer de clé personnelle

Le deuxième onglet du panneau d'options donne les caractéristiques de votre clé personnelle et offre un choix pour en changer.

La procédure est ensuite très similaire au choix initial de clé personnelle qui avait été fait lors de la toute première utilisation du logiciel (cf. §2.1.2)





Attention : la modification de la clé personnelle ne s'applique pas aux conteneurs déjà créés mais aux nouveaux conteneurs. En particulier pour changer le mot de passe d'un conteneur existant, il faut ouvrir la fenêtre des accès comme décrit au chapitre 2.5.3.

## 3. Messages d'erreur

Outre les messages d'erreur et d'avertissement relatifs au système d'exploitation Windows qui peuvent être émis lors des opérations sur les conteneurs (par exemple : « Impossible de renommer <nom du conteneur> : un fichier portant ce nom existe déjà. Spécifiez un nom différent. ») ou lors de la configuration des politiques de sécurité (valeurs interdites), des messages d'erreur spécifiques au produit Zed! informent l'utilisateur de problèmes rencontrés. Ces messages sont détaillés dans le tableau ci-dessous :

Messages d'erreur	Cause
Impossible de modifier les accès. Aucun accès n'est défini.	L'utilisateur tente de supprimer le dernier accès de la liste.
Le mot de passe est incorrect. Ce mot de passe est faux ou ne correspond pas à l'identifiant utilisateur fourni ...	Le mot de passe entré par l'utilisateur n'est pas valide.
Le mot de passe ne satisfait pas les critères de qualité requis.	Le mot de passe ne satisfait pas les contraintes minimales de longueur et de complexité (valeurs prédéfinies par l'administrateur de sécurité).
Ancien et nouveau mots de passe identiques	Lors d'un changement de mot de passe, le nouveau mot de passe entré par l'utilisateur est identique au précédent.
Le code d'accès du fichier de clés est incorrect	Le code d'accès du fichier de clé entré par l'utilisateur n'est pas valide.
Le format de ce fichier de clé est invalide ou non reconnu.	Le fichier utilisé lors de la création d'un accès n'est pas un fichier de clé.
Fichier d'accès invalide.	Le fichier d'accès est corrompu.
Aucune clé autorisée dans le fichier de clé.	Le certificat présenté par l'utilisateur n'est plus valide (date de validité incorrecte ou certificat révoqué).
Le code confidentiel de la carte/token est erroné	Le code confidentiel de la carte/token entré par l'utilisateur n'est pas valide.
Les clés trouvées dans la carte/token ne correspondent à aucune clé autorisée pour ce conteneur. Vous devez utiliser un autre moyen pour ouvrir le conteneur chiffré.	Les clés trouvées dans la carte/token ne sont pas valides.
L'accès sélectionné existe déjà.	L'utilisateur entre un identifiant déjà utilisé pour le nouvel accès.

Messages d'erreur	Cause
Impossible de créer le modèle de zone car un accès obligatoire défini dans les règles de sécurité n'a pas été trouvé.	La création du conteneur échoue car l'accès de recouvrement défini dans la politique P131 n'a pas été trouvé.
L'empreinte numérique (hash) d'un accès obligatoire n'a pas été trouvée, ou n'est pas bien formatée.  Les Règles de Sécurité doivent être vérifiées.	L'empreinte numérique a été incorrectement renseignée dans la politique P131.
La vérification de l'empreinte numérique (hash) d'un accès obligatoire a échoué.  Les Règles de Sécurité ou les fichiers concernés doivent être vérifiés.	L'empreinte numérique renseignée dans la politique P131 est incorrecte.
Un composant nécessaire du produit fait défaut. Vérifier l'installation.	Un composant du produit a été supprimé.
Le conteneur chiffré ne peut pas être lu avec cette version, une mise à jour est nécessaire.	La version utilisée ne permet pas d'ouvrir le conteneur créé par une version de Zed ! plus récente.



---

## 4. Notes