

Installation et emploi du logiciel de chiffrement ou signature de fichiers numériques Cryptonit

Menu	
•	Description
•	Installation
•	Ouverture
•	Configuration
○	Choix de la langue
○	Niveau de Cryptage
○	Autres réglages
▪	Répertoire par défaut
▪	Utiliser son certificat
▪	Profil de signature
▪	Ajouter un contact
•	Utilisation
○	Créer un fichier crypté exécutable
○	Ouvrir un fichier exécutable.
○	Autres utilisations
•	Recommandations
•	Liens internes
•	Liens externes
•	Droits d'auteurs

Description

Cryptonit est un logiciel très simple d'utilisation qui vous permettra de rapidement crypter des fichiers pour leur stockage ou l'envoi par e-mail et vous assurer ainsi une parfaite confidentialité.

Vous pouvez également utiliser Cryptonit pour crypter des fichiers que vous auriez à donner sur un support amovible: CD gravé, clé USB, etc.

Cryptonit génère des fichiers cryptés exécutables, il n'est ainsi pas nécessaire que le destinataire des fichiers installe de logiciel sur son ordinateur pour décrypter les fichiers reçus. Un simple double-clic sur le fichier crypté permet d'accéder via un mot de passe au fichier d'origine.

Cryptonit permet également de signer électroniquement vos documents si vous possédez un certificat, ou encore de vérifier l'authenticité de l'origine des fichiers que vous aurez reçu via les certificats.

Le cryptage/décryptage peut s'effectuer via un système de mot de passe ou via l'utilisation d'un certificat électronique.

Ces fonctions liées à l'utilisation d'un certificat électronique ne seront pas détaillées dans un premier temps dans ce tutorial.

Utilisé par de très grandes entreprises (Renaud, Total, AGF, Gan, Michelin, Sanofi Aventis, etc.) et les services gouvernementaux (CEA, MINEFI, Inserm, Mairie de Paris, etc.) Cryptonit est un outil professionnel dont la qualité n'est plus à démontrer.

Installation

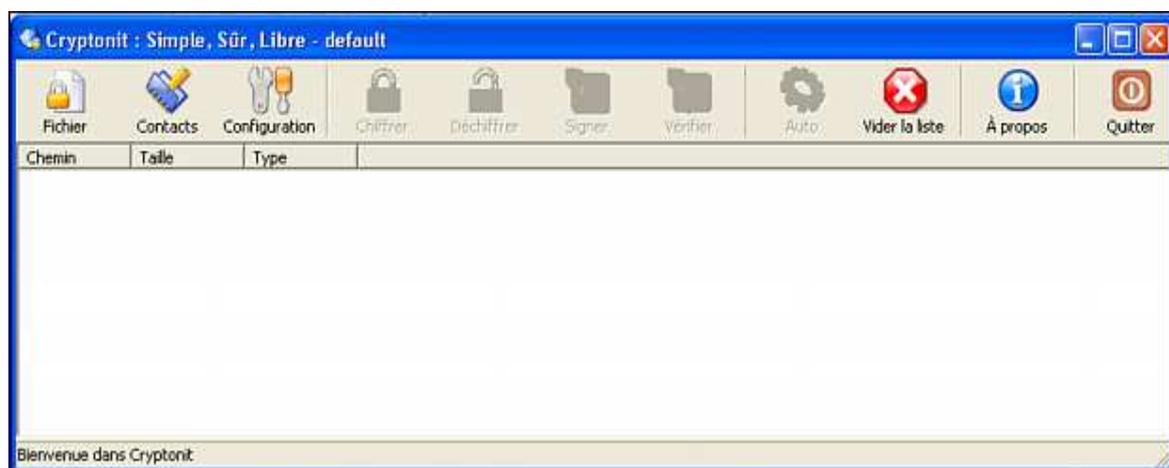
Cryptonit est un programme qui ne s'installe pas à proprement parlé sur votre ordinateur. C'est à dire qu'il vous suffit de double cliquer sur le fichier exécutable Cryptonit téléchargé pour l'ouvrir et l'utiliser. Cela veut dire également que vous pouvez très bien copier le programme Cryptonit sur un support amovible comme une clé USB par exemple afin d'avoir à portée de mains un utilitaire pour crypter vos documents.

Enregistrer le fichier sur votre disque dur. Par exemple sur votre bureau.

Ouverture

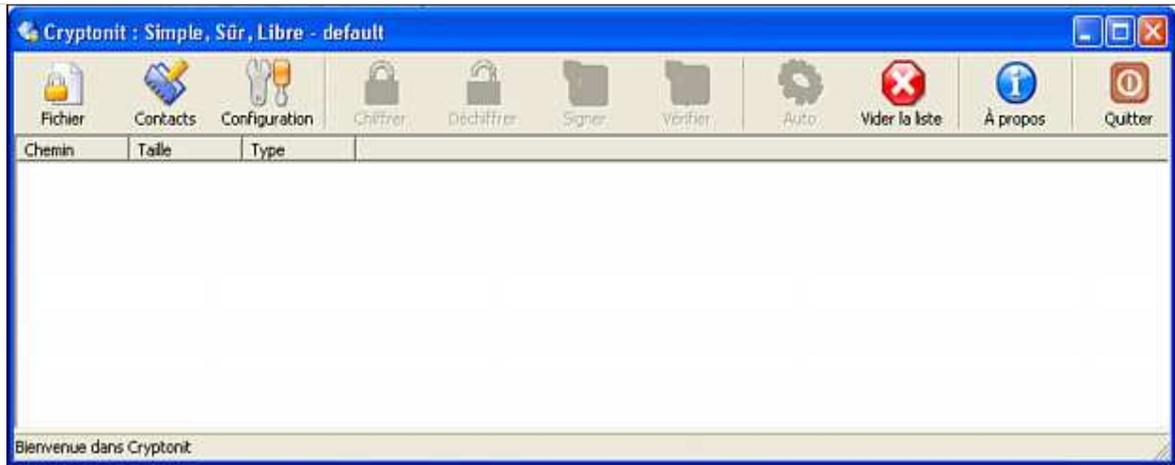


Comme indiqué ci-dessus, Cryptonit ne s'installe pas. Il suffit pour l'ouvrir de double cliquer sur le fichier téléchargé.



Ci-dessus la fenêtre principale de Cryptonit.

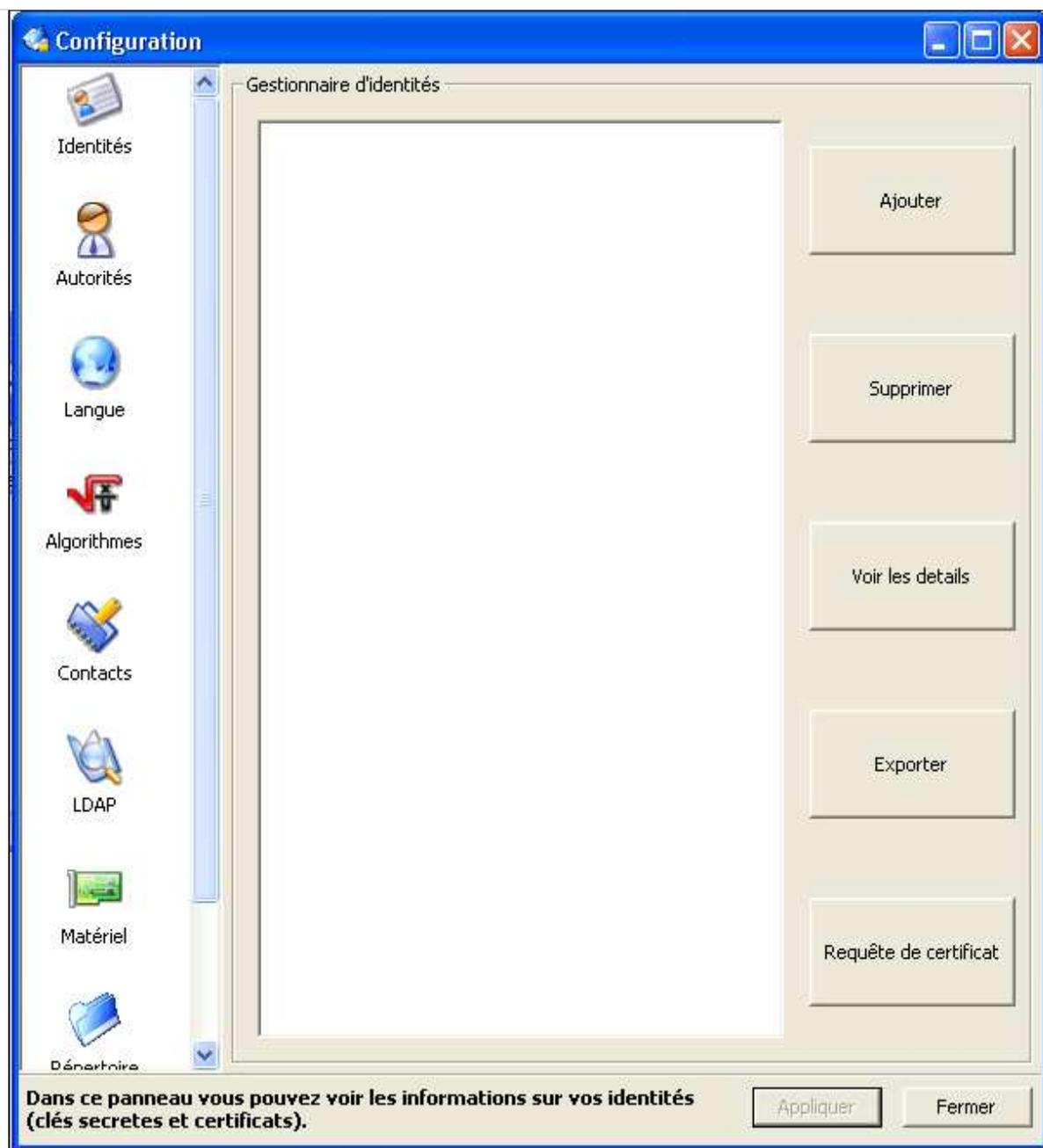
Configuration



Sur la fenêtre principale de Cryptonit ...



... cliquer sur configuration.



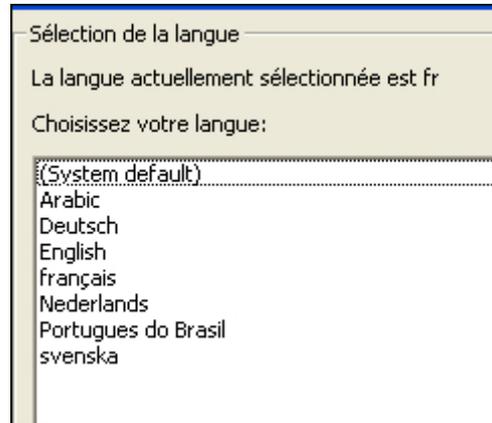
Ci-dessus, la fenêtre principale de configuration de Cryptonit. Pour une utilisation simple (génération de fichiers cryptés exécutables pour envoi par e-mail par exemple), seuls deux paramètres sont à modifier si le réglage d'origine ne vous convient pas: le langage de l'interface et le niveau de cryptage.

Les autres paramètres détaillés par la suite ne sont en prendre en compte que si vous voulez avoir une utilisation plus poussée de Cryptonit, par exemple pour signer à l'aide d'un certificat des fichiers. Attention, comme indiqué en introduction, les fonctionnalités poussées de Cryptonit ne seront pas décrites sous forme de tutorial ici dans un premier temps.

Choix de la langue



Pour régler la langue d'utilisation, cliquer sur l'option "Langue".



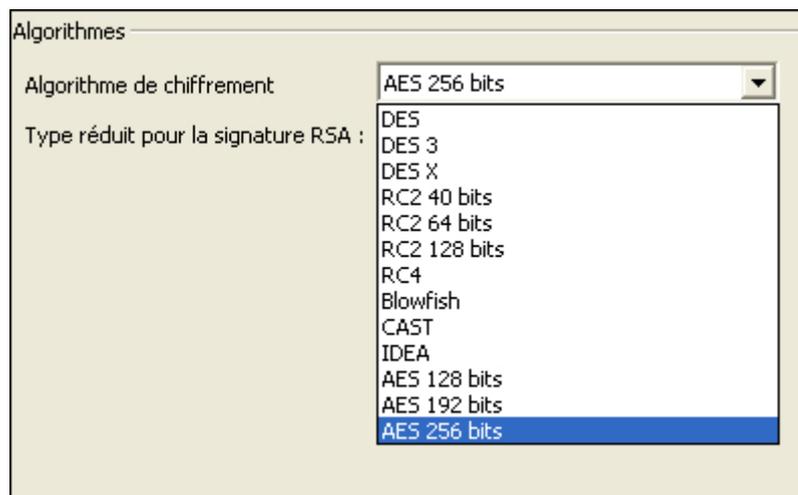
Choisir Français ou anglais en fonction des préférences.

Niveau de Cryptage



Le niveau de cryptage par défaut est réglé à AES 128 bits. Ce niveau, utilisé dans les systèmes bancaires, est largement suffisant. Vous avez cependant la possibilité de modifier ce niveau. Le temps de cryptage de vos fichiers sera cependant sensiblement plus long.

Cliquer sur "Algorithmes" ...



... puis dans le menu déroulant, choisir le niveau et le type de cryptage adéquat. Par exemple ici AES 256 bits.

Autres réglages

Répertoire par défaut



Avec l'option "répertoire par défaut", vous pouvez définir un dossier de votre ordinateur dans lequel vous déposez au fur et à mesure les fichiers que vous voulez cryptés. A l'ouverture de Cryptonit, vous pouvez demander au logiciel d'ajouter automatiquement tous les fichiers que vous aurez déposés dans ce dossier à la liste des fichiers à crypter.

Cliquer sur "Répertoire" ...



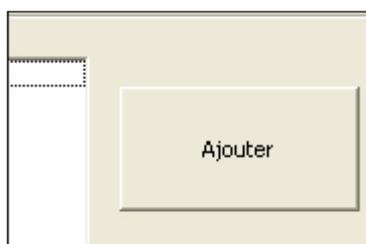
... et choisir le dossier voulu. Attention de bien cliquer sur "remplir automatiquement la liste ..." si vous souhaitez effectivement que Cryptonit rajoute dans la fenêtre principale les fichiers que vous aurez déposés dans le dossier par défaut.

Utiliser son certificat

Cryptonit permet de certifier un document donné via votre certificat de signature.



Pour cela, cliquer sur "Identités" dans le panneau de configuration.



Puis sur la droite, choisir l'option "Ajouter".



Importer comme indiqué votre certificat. Cliquer sur OK et suivre la procédure.

Profil de signature

Vous pouvez configurer par défaut d'attacher avec le fichier cryptée votre signature.



Cliquer sur "Profil de signature" ...



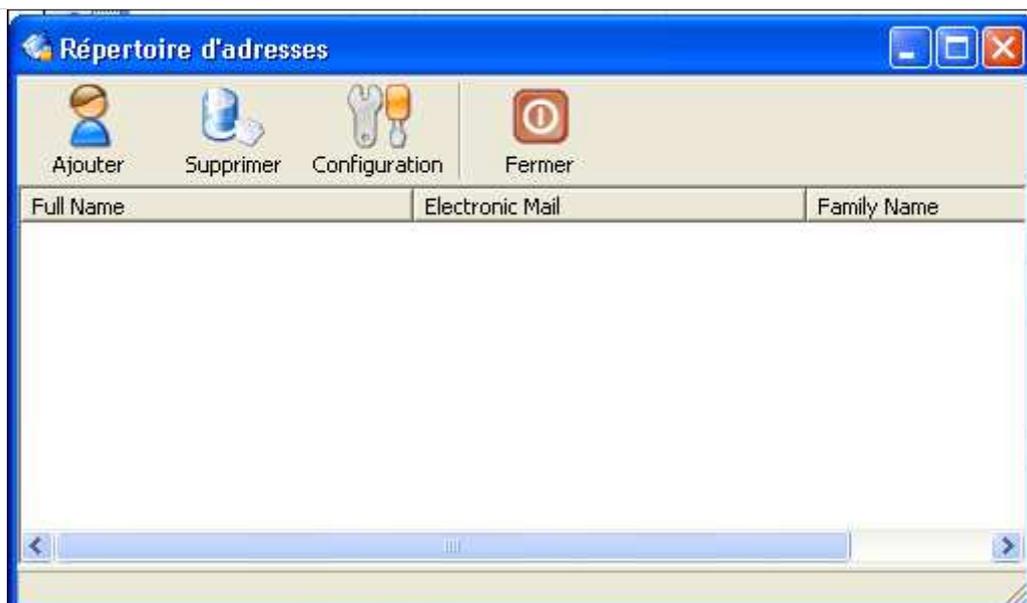
... et choisir "Attachée".

Ajouter un contact

Vous pouvez ajouter des contacts certifiés directement dans Cryptonit.



Pour cela, cliquer sur "Contact" au niveau de la fenêtre principale de Cryptonit.



Au niveau de la nouvelle fenêtre qui s'est ouverte ("Répertoire d'adresses")...



... choisir "Ajouter".



Importer le certificat du contact.



En cliquant sur configuration, vous pourrez choisir les champs à faire apparaître dans votre fenêtre "Répertoire d'adresses".



Faire passer de droite à gauche et vice versa les éléments que vous voulez voir affichés ou non. A gauche la liste complète des options disponibles, à droite les options qui apparaîtront dans votre fenêtre "Répertoire d'adresses".

Utilisation

Créer un fichier crypté exécutable



Dans la fenêtre principale de Cryptonit, cliquer sur "Fichiers".



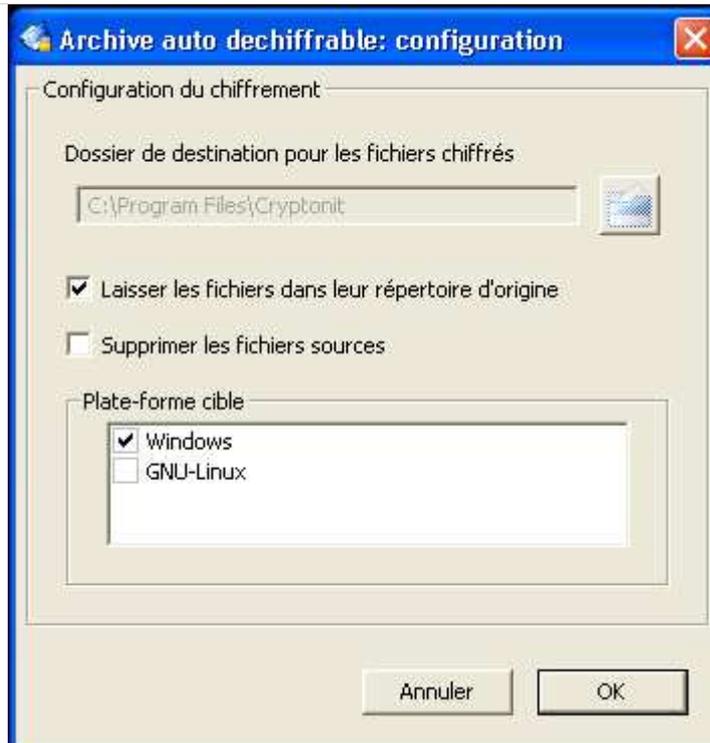
Alternativement, vous pouvez faire glisser le ou les fichiers à crypter dans la fenêtre principale de Cryptonit.

Remarque:

- Pour supprimer un fichier de la liste, cliquer dessus et utiliser la touche "Supprimer" ou "Del" de votre clavier.
- Attention, un fichier crypté sera créé par fichier d'origine. Voir les recommandations en bas de page pour crypter plusieurs fichiers en un seul.



Cliquer sur "Auto"



Dans cette nouvelle fenêtre, configurer les options suivantes:

- Chemin de destination du ou des fichiers cryptés (option non cliquable si l'option ci-dessous est sélectionnée)
- Répertoire d'origine: cocher cette option si vous voulez que le fichier d'origine soit généré dans le même dossier que celui du fichier à crypter.
- Suppression des fichiers sources: cocher cette option si vous voulez que le ou les fichiers d'origine soient supprimés de votre disque dur après génération du fichier crypter. Nous conseillons de ne pas cocher cette option et d'utiliser plutôt d'autres outils, comme par exemple [Eraser](#), pour supprimer définitivement le fichier d'origine si désiré.
- Plate-forme cible: cocher Windows si vous souhaitez pouvoir ouvrir le fichier généré crypté sur un ordinateur avec Windows. Cocher Linux pour un ordinateur sous Linux.



Entrer votre mot de passe. Attention, il ne sera plus possible d'ouvrir le fichier généré si vous perdez ce mot de passe. Pour une gestion efficace des mots de passe, utiliser [Keepass](#).

A l'invite, répéter le mot de passe choisi.



La vitesse de cryptage dépend de la taille du fichier d'origine. Une fois terminé, cliquer sur "Fermer".



Le fichier crypté généré possède le même nom que le fichier d'origine, avec en plus l'extension ".exe".

Ouvrir un fichier exécutable.



Double cliquer sur l'icône du fichier portant l'extension ".exe".



Dans la nouvelle fenêtre, indiquer le mot de passe.



Choisir le dossier de destination où sera enregistré le fichier à décrypter. Une fois validé, le dossier s'ouvrira automatiquement.

Autres utilisations

Cryptonit permet de crypter/décrypter ou signer et vérifier un fichier. Ces fonctions ne seront pas détaillées dans un premier temps dans le cadre de ce tutorial.



Cliquer sur les différentes options adéquates après avoir choisi le fichier à manipuler dans la fenêtre principale de Cryptonit.

Recommandations

- [Lire les recommandations sur le cryptage des données en entreprises](#)
- **Envoi par e-mail:** lors d'un envoi par e-mail, certains logiciels anti-virus peuvent reconnaître à tort les fichiers portant l'extension ".exe" comme des virus. Pour remédier à ce problème, deux solutions peuvent être envisagées:
 - retirer manuellement dans le nom du fichier le texte ".exe" et accepter la modification d'extension à l'alerte de Windows. Préciser ensuite à votre destinataire qu'il devra rajouter l'extension ".exe" dans le nom du fichier reçu pour rendre de nouveau exécutable/extractable le fichier en question.
 - **Plus simple:** "zipper" le fichier .exe avant son envoi, par exemple avec [7Zip](#), et envoyer à votre destinataire le fichier zippé.
- **Fichiers multiples:** pour ne faire qu'un seul fichier crypté à envoyer et contenant plusieurs fichiers d'origine, "zipper" au préalable ces fichiers en un seul fichier, puis crypter ce fichier unique "zippé". Pour "zipper" les fichiers, utiliser [7Zip](#).
- **Choix du mot de passe:**
 - utiliser un mot de passe pertinent et ne jamais le communiquer par e-mail, mais plutôt de préférence par téléphone après avoir clairement identifié la personne destinataire du fichier. Préciser également au destinataire de ne pas conserver le mot de passe communiqué sur un papier volant bien en évidence sur son bureau. Ne pas utiliser toujours le même mot de passe.
 - Pour le choix d'un mot de passe, vous pouvez vous aider de [Keepass](#).
- **Fichier d'origine à conserver ou non:**
 - attention de bien conserver une copie du fichier d'origine (par exemple au cas où vous perdriez le mot de passe pour ouvrir le fichier crypté). Pour conserver ce fichier de manière sécurisé, le stocker sur une partition cryptée via [Truecrypt](#).
 - Si vous souhaitez tout de même effacer le fichier d'origine, utiliser [Eraser](#) qui ne laisse aucune trace sur votre ordinateur.

o

Droits d'auteurs

Sauf indiqué, toutes images concernant Cryptonit: copyright Cryptonit/Opentrust.

Copyright CRVS 2008 - d'après un tutorial de Conseil POM

Créé par: [admin](#) dernière modification: Mardi 10 Mars, 2009 [13:57:10 UTC] par [christine.schmidt](#) 
