WebSphere MQ : Génération de certificats SSL auto-signés

Ce document présente la génération de certificats SSL auto-signés pour utilisation dans WebSphere MQ.

Principe

La mise en œuvre du chiffrement dans les channels WebSphere MQ nécessite l'utilisation de certificats SSL.

Ces certificats peuvent être de deux sortes :

- En provenance d'une *Certification Autority* (CA) comme Verisign, Globalsign, …
- Auto-signés, c'est à dire générés par l'utilisateur

Les certificats auto-signés ont peu d'intérêt pour l'authentification mutuelle des partenaires, par contre ils permettent de mettre en place une communication chiffrée par SSL sur le channel WebSphere MQ.

Accessoirement, ils sont aussi un bon moyen de valider une configuration en attendant la mise à disposition d'un certificat commandé à une CA.

L'outil *IKeyMan* (IBM Key Management) est livré avec de nombreux produits IBM et Tivoli, et permet la gestion des certificats SSL, y compris les certificats auto-signés. Cet outil est par exemple disponible après l'installation de l'IBM HTTP Server (IHS).

Le site de l'IHS : http://www-3.ibm.com/software/webservers/httpservers/

Lancement de IkeyMan et création de la base de clés

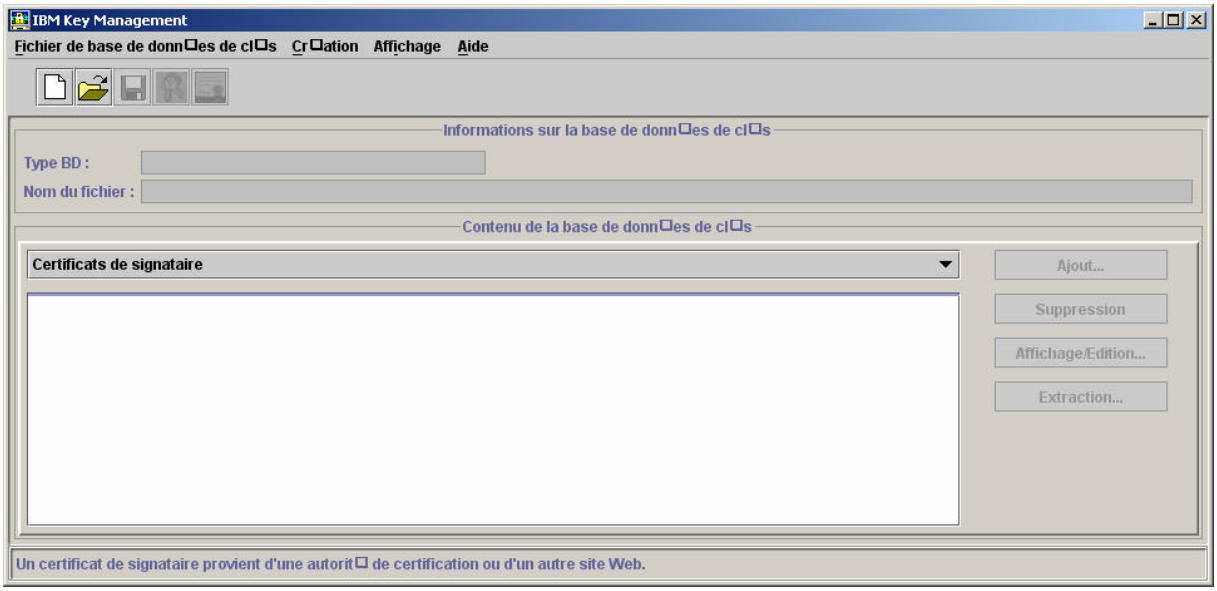
La base de clés contient l'ensemble des clés et certificats générés et reçus au niveau d'un système. Il est tout à fait possible de créer l'ensemble des certificats sur un système, puis d'exporter ceux-ci vers les machines qui utiliseront ce ou ces certificats.

- Sous Unix, on lance "***ikeyman***" sur la ligne de commande.
- Sous Windows, "*Démarrer/Programmes/IBM HTTP Server/Démarrage de l'utilitaire IBM Key Management* "

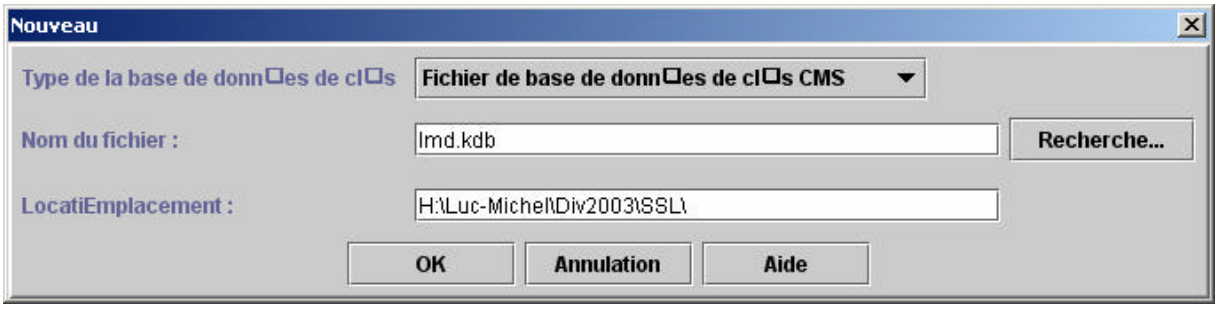
On obtient une applet Java comme ceci :

Contact : ftwmq2006@demey-consulting.fr - http://demey-consulting.fr

WebSphere MQ : Génération de certificats SSL auto-signés



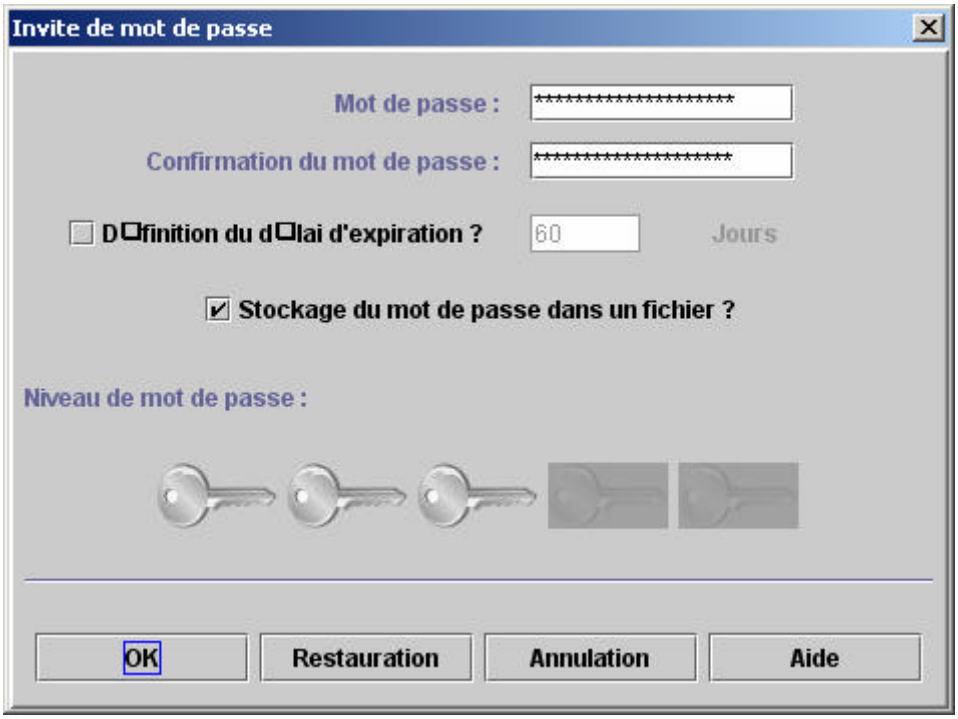
Lors de la première utilisation, il est nécessaire de créer la base de clés par *" Fichier de base de données/Nouveau* " :



Préciser les champs suivants :

- Type de la base : "*Fichier de base de données de clés CMS*" (défaut)
- Nom du fichier : garder le défaut "*key.kdb*" ou préciser un nom en ".kdb"
- Emplacement : préciser un emplacement ou garder le défaut (répertoire de l'IBM HTTP Server). Dans tous les cas, penser à noter le nom et l'emplacement de la base.

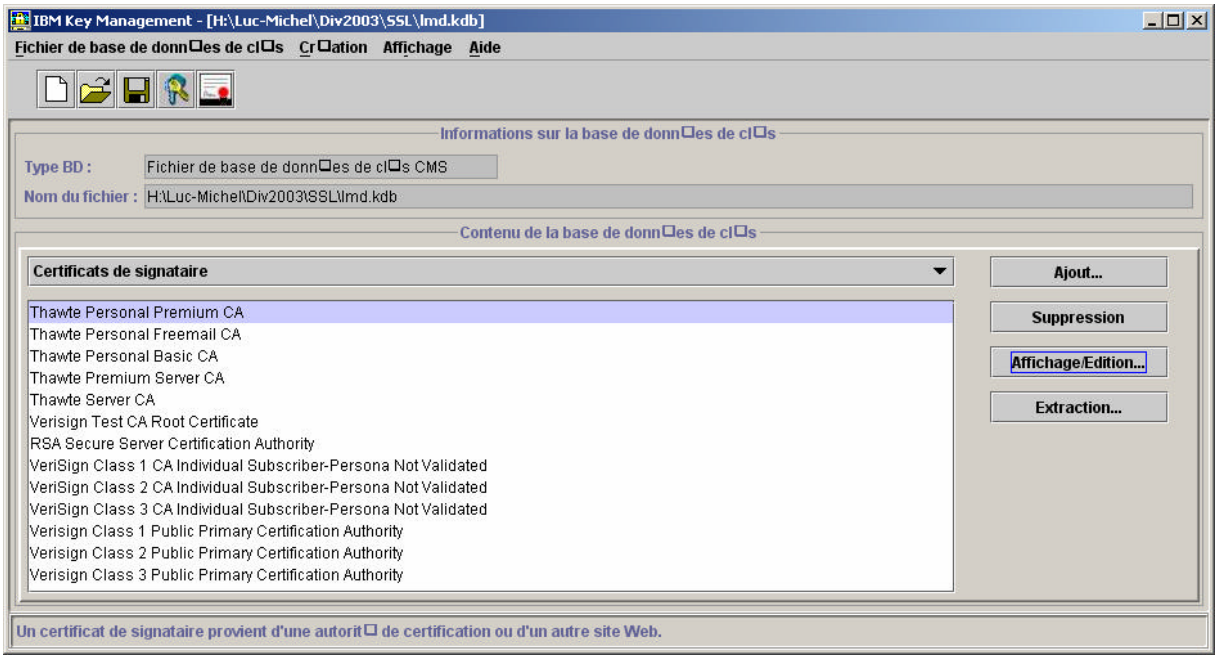
WebSphere MQ : Génération de certificats SSL auto-signés



- Mot de passe : il s'agit du mot de passe qui protège la base de clés et donc les clés privées des certificats. Notez-le avec le nom et l'emplacement de la base de clés.
- Stockage du mot de passe dans un fichier : cocher cette case

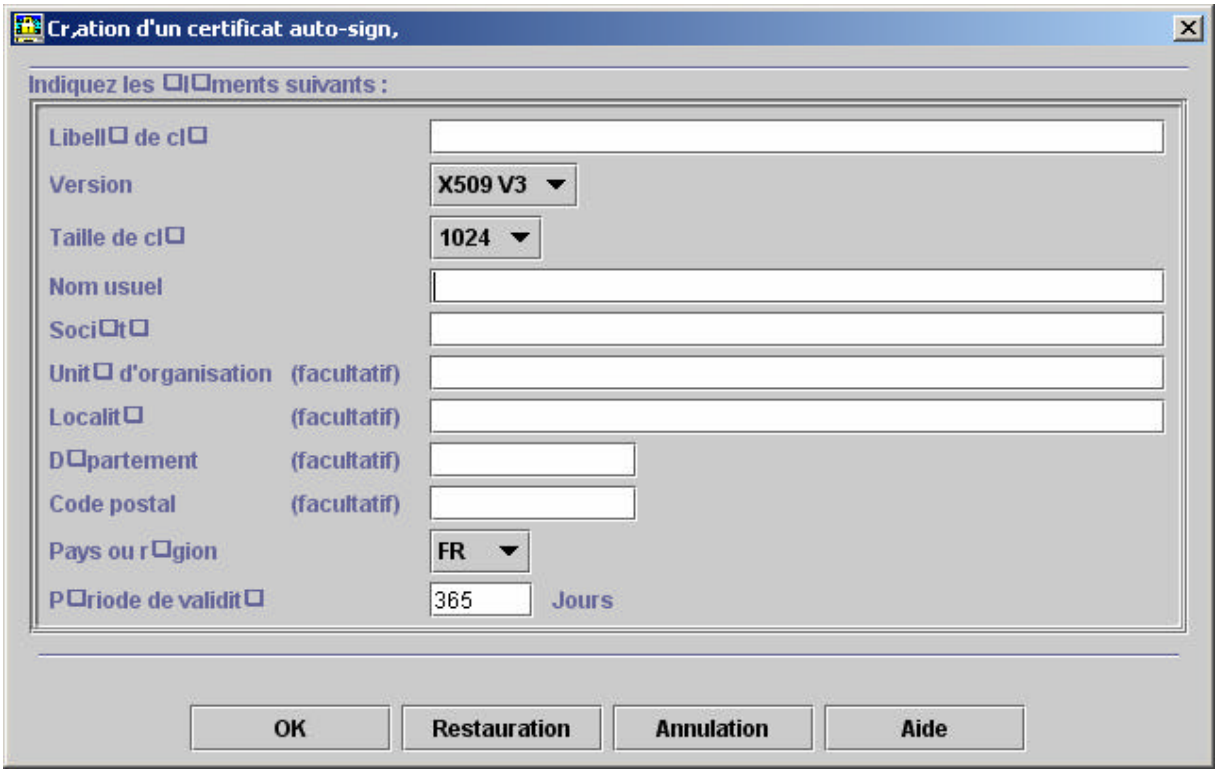
On obtient ensuite l'écran de gestion de la base, ouvert à l'onglet des certificats "racine" :

WebSphere MQ : Génération de certificats SSL auto-signés



Création d'un certificat auto-signé

Cliquez sur l'icône  (ou choisissez "*Création/Nouveau Certificat auto-signé*") :



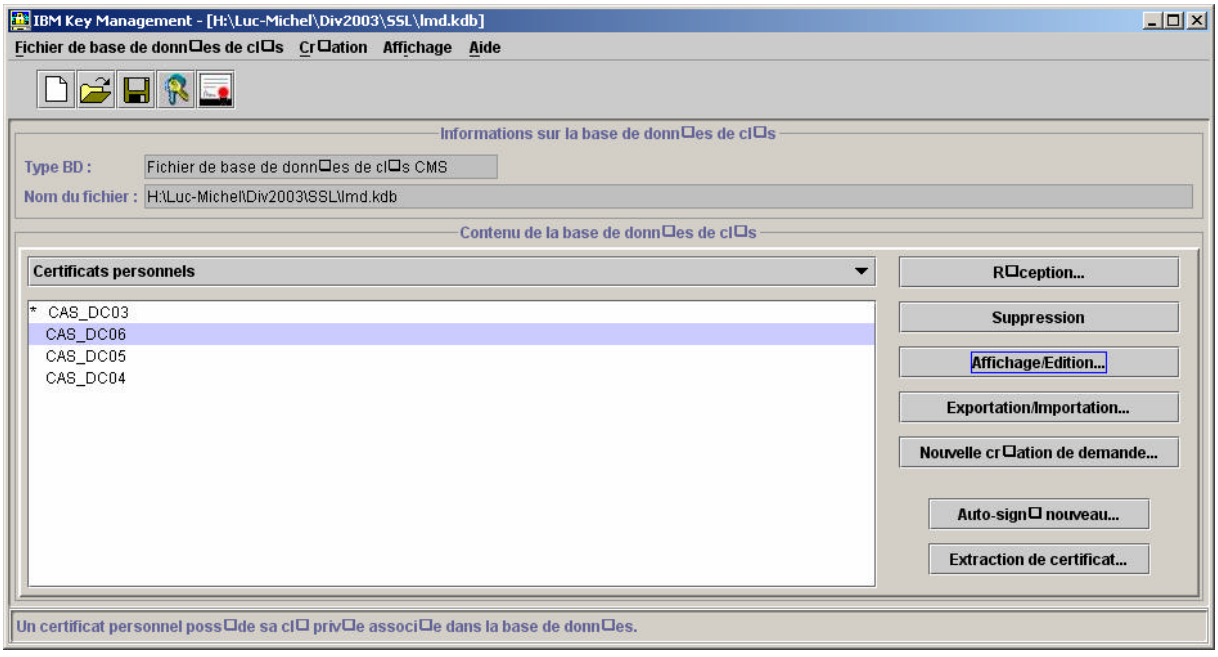
Contact : ftwmq2006@demey-consulting.fr - http://demey-consulting.fr

WebSphere MQ : Génération de certificats SSL auto-signés

Renseignez les zones comme suit :

- Libellé de clé : Nom que vous souhaitez donner à votre certificat (par exemple CAS_DC06)
- Version / Taille de clé : laisser les valeurs par défaut (X509 V3 / 1024)
- Nom usuel : dans le cas d'un certificat destiné à un serveur Web, ce nom doit correspondre au nom qualifié du serveur. Pour WebSphereMQ, vous pouvez indiquer le nom du QM où ce certificat sera utilisé.
- Société : Le nom de votre société (facultatif)
- Période de validité : par défaut, ce certificat sera valable 365 jours, ce qui est trop ou trop peu. S'il s'agit d'un test de courte durée, indiquez 30 ou 60 jours. S'il s'agit d'un certificat auto-signé destiné à être utilisé en production, assurez-vous qu'il existe une procédure de renouvellement de ce certificat. Sinon, indiquez une durée très longue (3650 jours ?)

On obtient ensuite la liste des certificats existants dans la base :



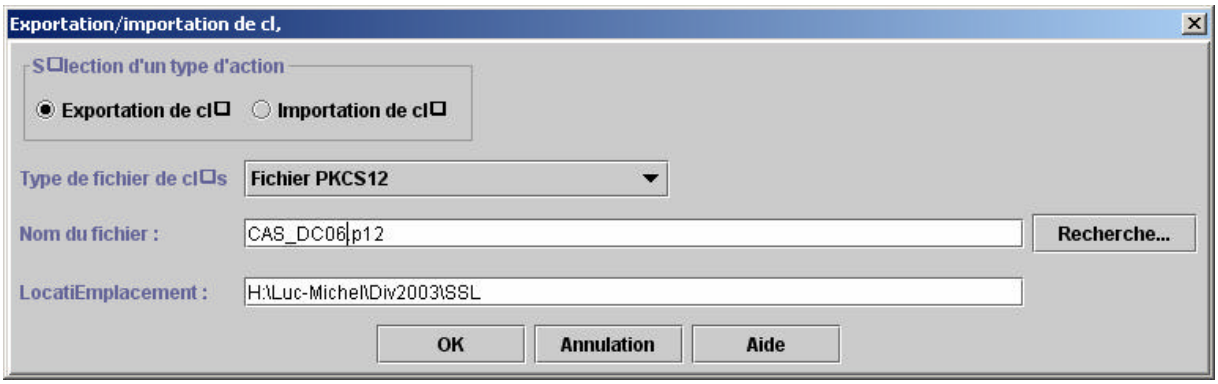
Exportation d'un certificat

Dans cet exemple, la base de clés a été crée sur la machine YETI. Pour être utilisés avec WebSphere MQ, ces certificats devront être importés dans le référentiel de clés correspondant de la machine utilisant SSL. La première chose à faire est donc d'exporter le ou les certificats créés, sous la forme d'un fichier "pk12".

Par exemple, pour exporter le certificat CAS_DC06, procédez ainsi :

WebSphere MQ : Génération de certificats SSL auto-signés

- Cliquez à droite sur le bouton "*Exportation / Importation*"
- Dans l'écran suivant, précisez :
  - Le type d'action (*exportation*)
  - Le type de fichier de clé à utiliser pour l'exportation (garder la valeur par défaut PKCS12)
  - Le nom et l'emplacement du fichier d'export



Le système vous demande ensuite le mot de passe permettant ce chiffrer ce fichier et le type de chiffrement à utiliser. Garder la valeur par défaut "*chiffrement fort*".

Vous pouvez ensuite transfèrer, par tout moyen à votre convenance, le fichier contenant le certificat vers le système cible et/ou l'importer dans le référentiel de clés de WebSphere MQ.

Fin du document

Contact : ftwmq2006@demey-consulting.fr - http://demey-consulting.fr