Auditiel

EJBCA

PKI Open Source

Manuel d'installation et de configuration

Version 1.0.0

http://www.auditiel.fr/docs/EJBCAInstallation.pdf
Référence : 1.3.6.1.4.1.28572.1.2.2.1.1

1 SOMMAIRE

2 INTRODUCTION

2.1 Pré requis

Ce document s'adresse aux personnes désirant installer une PKI d'entreprise. Il est nécessaire d'avoir un minimum de connaissance sur le fonctionnement des PKI et sur l'utilisation des certificats.

2.2 Versions

Version	Date	Auteur	Modification
1.0.0	22/02/2007	Jérôme DUSAUTOIS	**Création**

2.3 Glossaire

CA : Autorité de certification.

CA Root : Autorité de certification racine. Cette autorité est signée par elle-même (auto-signée). Aucune autre autorité ne se porte garante de sa validité.

SubCA : Sous autorité de certification, dépend d'une autre sous autorité ou d'une autorité racine.

RA : Autorité d'enregistrement. Prend en charge l'inscription des utilisateurs finals et l'enregistrement des demandes de certificats.

JAVA : Langage de programmation multi plateforme.

JDK : Outils de développement des applications JAVA, pour une plateforme donnée.

JBOSS : Serveur d'applications en JAVA.

EJBCA : PKI Open Source en JAVA, basée sur le serveur d'applications JBOSS.

3 INSTALLATION

3.1 Composants nécessaires

L'installation et l'utilisation d'EJBCA nécessitent le chargement de plusieurs composants. Voici un tableau des composants à charger, ainsi que l'adresse Internet où vous les trouverez.

Modules	Version	Adresse
EJBCA	3.4.1	**www.ejbca.org**
Serveur JBOSS	4.0.4	**labs.jboss.com**
Installeur ANT	1.7.0	**jakarta.apache.org/ant/**
JDK SUN	1.5	**java.sun.com/j2se/1.5.0/download.jsp**
JCE Policy	1.5.0	**java.sun.com/j2se/1.5.0/download.jsp**
MySQL (optionnel)	5.0	**www-fr.mysql.com**
MySQL JAVA connector	**5.0.4**	**www-fr.mysql.com**

3.2 Système d'exploitation

EJBCA est une PKI réalisée en JAVA. Tous les composants utilisés fonctionnent en JAVA ou existent sur plusieurs plateformes.

Le fonctionnement d'EJBCA est identique (sauf avis contraire), sur toutes les plateformes.

La procédure d'installation décrite ici, est réalisée sur une plateforme Windows. Les commandes exécutées sont donc des commandes CMD. Les mêmes commandes, avec l'extension SH, existent pour Linux.

3.3 Installation en production

La base de données intégrée à JBOSS ne permet pas une exploitation confortable à long terme. En effet, Hypersonic est une base de données qui charge ses tables en mémoire. Cette configuration ne peut pas fonctionner longtemps en production.

Il est préférable d'utiliser une base SQL externe. JBOSS supporte les bases suivantes : mySQL, PostgreSQL, Oracle, Sybase, SapDB, MSSQL.

Reportez-vous à la partie .

3.4 Procédure d'installation

Suivez les étapes ci-dessous pour réaliser l'installation d'EJBCA. Dans la suite de la procédure, on considère que tous les composants nécessaires ont été téléchargés.

1. Copier les répertoires Apache-ant-1.7.0-bin, JBoss-4.0.4.GA, JDK_1.5.0_11 et EJBCA_3_4_1 dans le répertoire d'installation *repinstall*.

2. Si vous désirez utiliser MySQL, c'est le moment de suivre les étapes de la partie suivante ().
3. Ajouter, dans la variable d'environnement PATH, le chemin aux exécutables de ant (*repinstall*\Apache-ant.1.7.0-bin\bin) et JAVA (*repinstall*\JDK_1.5.0_11\bin).
4. Ajouter la variable d'environnement JAVA_HOME avec le chemin du JDK. (*repinstall*\jdk.1.5.0_11).
5. Ajouter une variable d'environnement JBOSS_HOME avec le chemin d'accès à JBOSS (*repinstall*\jboss-4.0.4.GA).
6. Copier les fichiers US_Export_Policy.jar et local_policy.jar du répertoire jce_policy-1.5.0 vers le répertoire jdk_1.5.0_11\jre\lib\security
7. Copier le fichier conf/ejbca.properties.sample en conf/ejbca.properties et le modifier si nécessaire (nom de la CA Root, taille des clés, mots de passe, durée de validité, …). Modifier, dans ce même fichier, les mots de passe pour les magasins de clés CA, OCSP, CMS. Ce fichier devra être sauvegardé en lieu sûr et supprimé du répertoire après l'installation.
8. Ouvrir une session de commande dans le répertoire *repinstall*\ejbca_3_4_1 et entrez la commande 'ant bootstrap'
9. Ouvrir une autre session de commande dans *repinstall*\jboss-4.0.4.GA\bin et lancer la commande run, pour activer le serveur JBOSS
10. Dans la session de commande EJBCA, lancer 'ant install'. Entrer le nom de DN et les mots de passe demandés.
11. Arrêter le serveur JBOSS par Ctrl+C
12. Dans la session de commande EJBCA, lancer 'ant deploy'
13. Importer le p12 superadmin.p12 du répertoire *repinstall*\jbca_3_4_1\p12 dans le magasin Windows.
14. Relancer le serveur JBOSS (run).
15. Connectez-vous avec le browser à l'adresse http://localhost:8080/ejbca. Le choix Administration permet d'accéder à l'interface WEB d'administration.
16. N'oubliez pas de sauvegarder et supprimer le fichier ejbca.properties du répertoire ejbca_3_4_1\conf. Ce fichier contient les mots de passes des magasins de clés.

3.5 Installation de la base MySQL

Ces étapes doivent être réalisées avant l'installation d'EJBCA, mais après avoir copié les fichiers dans le répertoire d'installation. Suivez les étapes ci-dessous.

1. Installez MySQL 5 en utilisant l'installeur. Sélectionnez la configuration 'typique'.
2. Passez la phase d'enregistrement sur Internet.
3. Laissez actif le lancement de la configuration MySQL. Le configurateur se lance automatiquement à la fin de l'installation. Sinon, vous pouvez

toujours lancer le configurateur par la commande MySQLInstanceConfig.exe dans le répertoire bin d'installation de MySQL.

4. Choisissez la configuration détaillée.
5. Indiquez qu'il s'agit d'une machine serveur.
6. Sélectionnez 'base de données transactionnelle uniquement'.
7. Changez éventuellement le chemin d'installation des bases.
8. Laissez le choix par défaut pour le nombre de connexions concurrentes.
9. Autorisez les connexions TCP/IP, mais pas pour l'administration.
10. Sélectionnez le support multi langues (UTF8).
11. Sélectionnez l'activation en tant que service Windows ainsi que l'ajout dans le PATH du chemin d'accès au répertoire BIN.
12. Modifiez le mot de passe root avec une valeur complexe.
13. Exécutez la configuration. Il se peut qu'un message d'erreur apparaisse, sélectionnez le bouton Retry et tout doit fonctionner. MySQL est prêt et actif.
14. Recopiez le fichier MySQL-connector-java.5.0.4-bin.jar, extrait du zip MysSQL-Connector-java, dans le répertoire JBOSS-4.0.4.GA\server\default\lib.
15. Copiez le fichier conf/database.properties.sample en conf/database.properties dans le répertoire ejbca_3_4_1\conf. Editez le fichier et enlevez les commentaires sur les lignes concernant la base de données MySQL (database.name, datasource.mapping, database.url, database.driver). Modifiez également le nom d'utilisateur et le mot de passe associé (database.username, database.password). Le nom d'utilisateur et le mot de passe sont créés dans le point suivant.
16. Lancez une session de commande et tapez les commandes suivantes.

```
Mysqladmin -uroot -ppasswordroot create ejbca
Mysql -uroot -ppasswordroot MySQL
grant all on ejbca.* to username@localhost identified by password
quit
```

Où

Root et *passwordroot* correspondent à l'identifiant et au mot de passe de l'utilisateur principal de la base de données.

Et

Username@localhost et *password* correspondent à l'identifiant et au mot de passe inscrits dans le fichier database.properties respectivement dans les champs database.username et database.password.

3.6 Sécurisation de l'installation

Pour une installation en production, les points suivants doivent être modifiés :

1. Sécurisez le serveur JBOSS en désactivant les consoles d'administration (JMX et WEB). Voici un lien sur un document qui explique la procédure : http://wiki.jboss.org/wiki/Wiki.jsp?page=SecureTheJmxConsole
2. Supprimez les autorités reconnues dans le magasin cacerts de la jre de SUN et ne laissez que le certificat de l'autorité créé par EJBCA pour l'administration. Pour cela, supprimez le fichier cacerts avant de lancer la commande ANT Install.
3. Bloquez tous les ports par défaut de JBOSS et ne laissez que les ports https 8442 pour l'interface publique et 8443 pour l'administration. Attention, la CRL est, par défaut, accessible sur le port http 8080.
4. Laissez l'accès aux fichiers du serveur JBOSS uniquement au compte utilisé pour lancer le serveur. Même remarque pour la base de données, s'il ne s'agit pas de la base intégrée à JBOSS.
5. Vérifiez que les logs de la base de données soient désactivées.

4 CONFIGURATION INITIALE

4.1 Première CA

La première CA Root a été créée lors de l'installation. Cette CA peut servir pour la production, si les informations ont bien été modifiées dans le fichier ejbca.properties avant l'installation d'EJBCA.

Elle peut également ne pas être utilisée pour la production si, par exemple, la CA de production dépend d'une autre CA.

Dans tous les cas, la CA créée lors de l'installation sert à authentifier le super administrateur.

Si pour une raison propre à l'organisation, une autre CA Root devait être utilisée pour générer les certificats d'authentification pour l'administration d'EJBCA, alors le certificat de l'autorité devrait être ajouté aux certificats reconnus par la JRE de SUN, dans le magasin cacerts qui se trouve dans le répertoire *RepInstall*\jdk1.5.0_11\jre\lib\security.

Les deux commandes suivantes permettent de récupérer le certificat de la CA Root et de l'importer dans le magasin des autorités reconnues par la JRE.

```
Ejbca ca getrootcert NomCA nomfichierca.crt -der

Keytool -import -trustcacerts -alias NomCA -keystore NomKeyStore -storepass
MotDePasse -file NomFichierCA.crt
```

Par défaut, le mot de passe du magasin de certificats reconnus de la JRE de SUN est *changeit*. Comme son nom l'indique, ce mot de passe doit être changé.

Le fichier *RepInstall*\jdk1.5.0_11\jre\lib\security\cacerts est, par défaut, le fichier contenant les certificats reconnus *(NomKeyStore).*

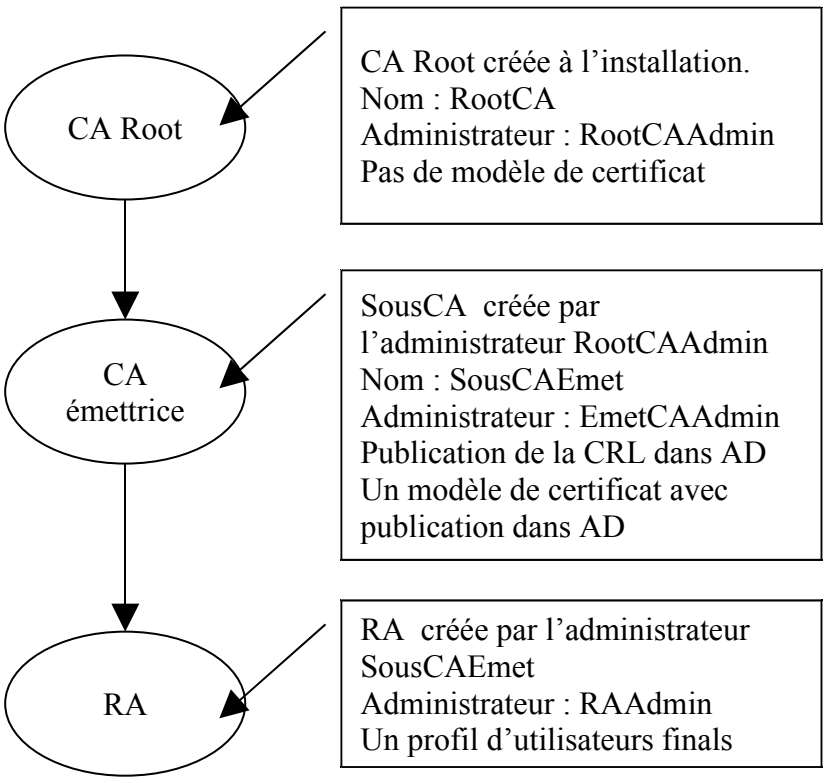
5 CONFIGURATION DE TEST

5.1 Présentation

Ce chapitre traite de la configuration d'EJBCA pour une PKI comportant une CA Root, une CA émettrice et une RA.

Avant de configurer la PKI, il est indispensable de bien spécifier l'ensemble des modules à créer (CA, SousCA, Publication, RA). Il faut également définir les groupes d'administrateurs pour chacun des modules. N'hésitez pas à donner des noms les plus explicites possibles pour les différents modules de la PKI. La compréhension n'en sera que meilleure.

Les administrateurs peuvent faire partie de la CA de production, ou une CA spécifique (par exemple, celle créée lors de l'installation). Cette dernière ne sera utilisée que pour l'administration. Dans notre exemple, les administrateurs font partie de la CA de production. La CA Root est créée lors de l'installation.



Remarque : Il n'y a pas vraiment de module RA. La RA est créée lorsqu'un groupe d'administrateurs a les autorisations de RA et qu'un profil d'entité final lui est associé.

5.2 Connexion au module d'administration

Connectez-vous sur le serveur JBOSS à l'adresse http://*nomduserveur*:8080/ejbca.

Ecran 1 : Page d'accueil

Sélectionnez le choix Administration.

La connexion au module d'administration nécessite un certificat d'authentification. Ce certificat a été créé lors de la phase d'installation. Le fichier p12 contenant le certificat et la clé privée est placé dans le répertoire *repinstall*\ejbca_3_4_1\p12 sous le nom SuperAdmin.p12. Il doit être installé dans votre navigateur.

Ecran 2 : Interface d'administration du Super Administrateur

5.3 Configuration du système

Sélectionnez le choix « System Configuration » pour modifier les paramètres du système. Les paramètres du système sont présentés sur deux pages. Les paramètres suivants peuvent être modifiés :

- Titre de l'application.
- Bannières haute et basse.
- Limitation des autorisations sur les entités finales.
- Utilisation du séquestre des clés.
- L'utilisation de supports physiques.
- Demander la confirmation pour l'envoi des mails de validation.
- La langue d'affichage.
- Le nombre de lignes par page.

Ecran 3 : Première page des paramètres du système

5.4 Création des interfaces de publication

Les interfaces de publication doivent être créées en premier, car elles peuvent être utilisées par les CA. Cependant, rien n'interdit la création d'interface de publication ultérieurement.

Pour créer une interface de publication, sélectionnez le choix « Edit Publishers », entrez un nouveau nom pour l'interface et sélectionnez le bouton « Add ». Sélectionnez ensuite le nom dans la liste puis le bouton « Edit Publisher ».

Nous devons créer deux interfaces de publication, une pour la CRL, utilisée et paramétrée par la CA émettrice et l'autre pour les certificats, utilisée également par la CA émettrice mais paramétrée dans le modèle de certificat. Elles portent respectivement les noms de CRL Publisher et AD Publisher.

Ecran 4 : Interface de publication

Les deux interfaces de publication utilisent le même type : Active Directory Publisher.

Elles utilisent également le même compte de sécurité Active Directory pour enregistrer les informations : Administrateur. Attention, il faut créer un compte spécial qui ne sera utilisé que par EJBCA. Ce compte doit avoir les autorisations pour modifier, voire créer, les entrées Active Directory correspondant aux utilisateurs ou à la CRL.

L'inscription dans Active Directory se fait dans l'enregistrement correspondant au DN composé d'une base et d'un champ complémentaire obtenu à partir du certificat à enregistrer dans la base.

La base DN pour l'inscription des certificats utilisateur dans AD est : CN=users,DC=dmn1,DC=fr.

La base DN pour l'inscription des CRL est : CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=dmn1,DC=fr

Le nom du domaine est ici dmn1.fr

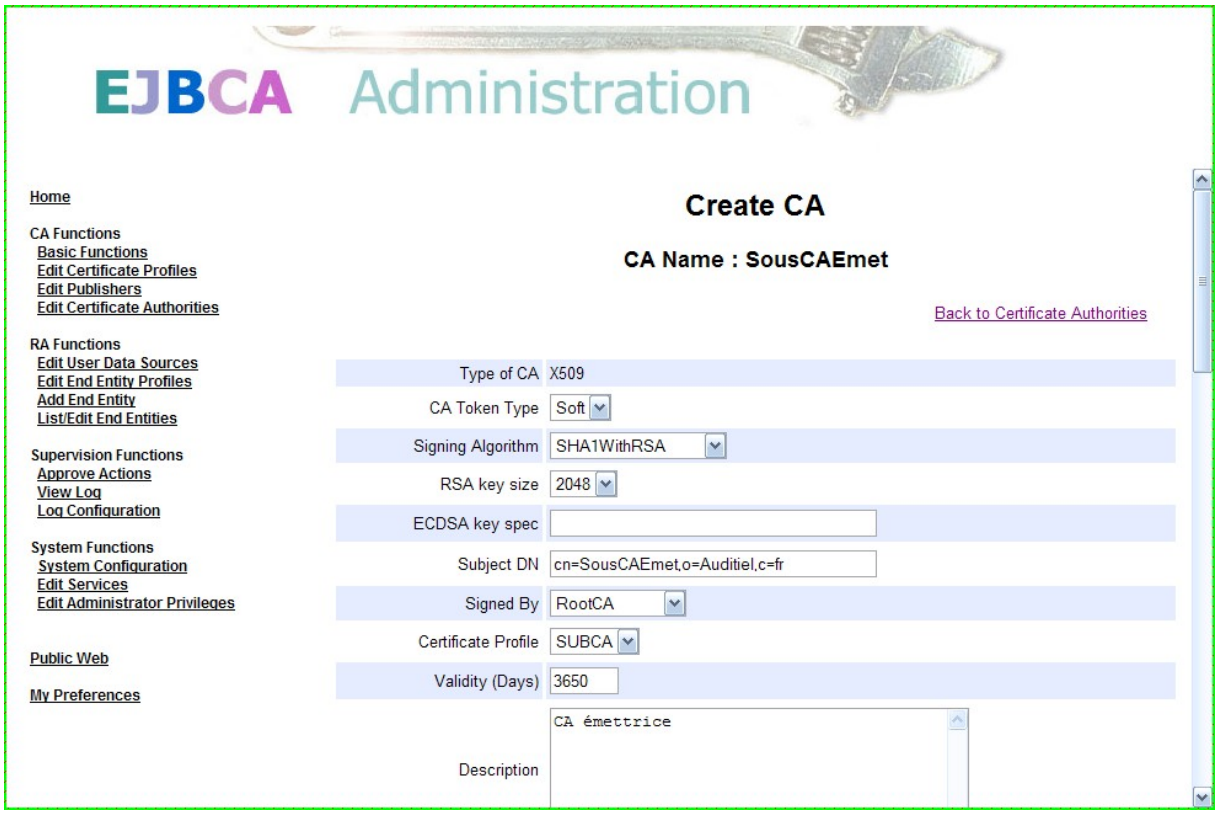
A cette base DN, sera ajouté le CN du certificat. Le tout correspond à l'entrée Active Directory à mettre à jour.

D'autres paramètres permettent de déterminer si les utilisateurs doivent être ajoutés dans Active Directory.

5.5 Création de la CA subordonnée

Cette SousCA est utilisée pour la génération des certificats utilisateurs.

Sélectionnez le choix « Edit Certificate Authorities », entrez le nom de la sous CA et sélectionnez le bouton « Create ».



Ecran 5 : Ajout de la CA émettrice

Sélectionnez la taille de la clé, la CA dont dépend cette sous CA et le délai de validité de la CA. Vous devez également fournir un dn.

Vous pourrez ensuite sélectionner l'interface de publication à utiliser (CRL Publisher créée précédemment).

Vous devez entrez un nombre d'heures de validité de la CRL. Vous pouvez également saisir l'URL d'accès à la CRL. Le bouton « Générer » permet de pré remplir le champ avec l'adresse du serveur et le dn de la CA. N'oubliez pas de modifier l'adresse du serveur, car par défaut l'adresse est « localhost ».

Cette adresse de CRL sera utilisée comme valeur par défaut, lors de la génération des certificats.

Lorsque tous les champs sont renseignés, sélectionnez le bouton « Save » pour enregistrer les paramètres et créer la CA. Cette opération peut prendre un peu de temps, en fonction de la taille des clés à générer.

Le modèle de certificat utilisé est le modèle créé automatiquement à l'installation d'EJBCA. Ce modèle (SUBCA) ne peut pas être modifié.

5.6 Création du modèle de certificat

Sélectionnez le choix « Edit Certificate Profiles », entrez un nouveau nom pour le profil, sélectionnez le profil « End User » dans la liste et sélectionnez le bouton « Use selected as template ». Ceci permet de copier le modèle de certificat « End User ».

Ecran 6 : Ajout d'un modèle de certificat

Le modèle de certificat permet de définir les informations suivantes :

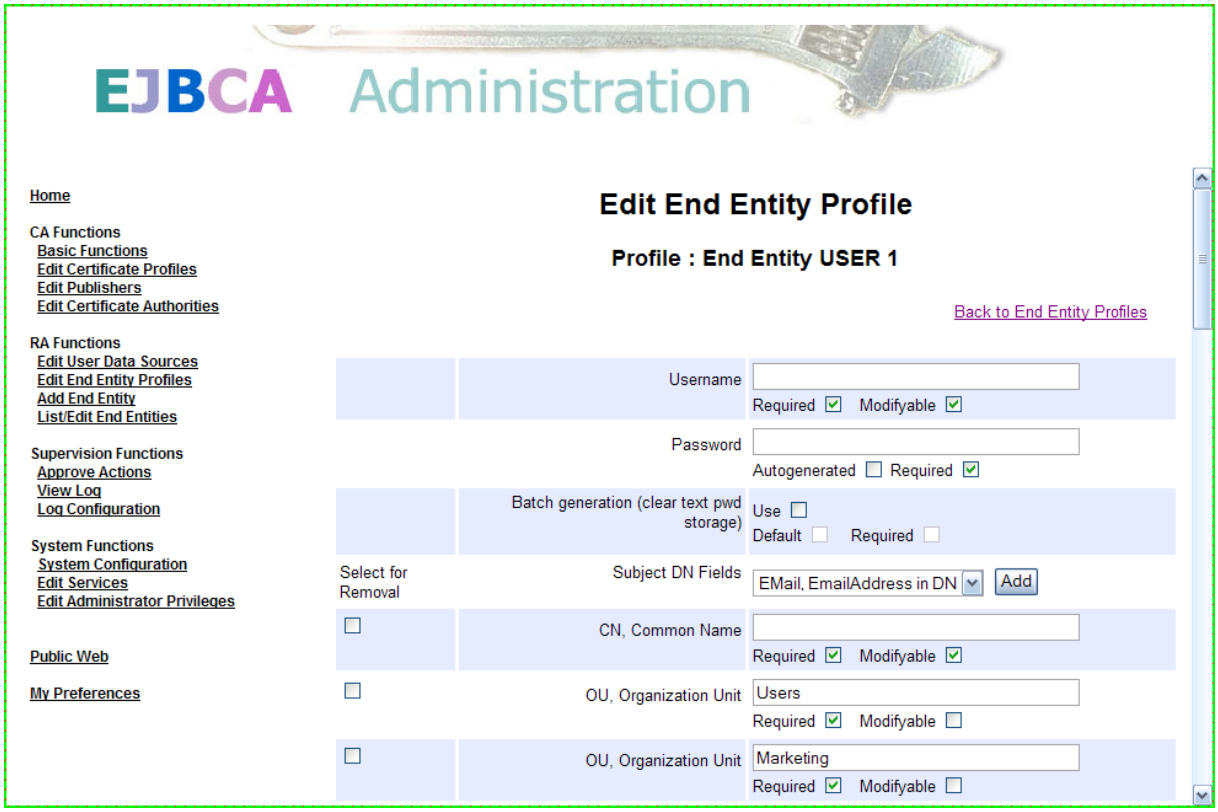
- Le délai de validité des certificats générés sur ce modèle.
- La présence et la criticité des attributs du certificat comme le « Key Usage », l' « Alternate Key Usage », le « Subject Alternative Name », l'adresse de la CRL, l'adresse du serveur OCSP, et bien d'autre…
- L'utilisation de la clé, en sélectionnant le ou les rôles prévus pour ce certificat.
- Les tailles de clés autorisées.
- La ou les CA qui peuvent délivrer ce modèle de certificat. Sélectionnez la Sous CA nouvellement créée : « SousCAEmet ».
- La ou les interfaces de publication à utiliser. Sélectionnez « AD Publisher »

Sélectionnez le bouton « Save » pour créer le modèle.

5.7 Création des profils

Nous devons créer deux profils. Le premier pour les administrateurs et le second pour les utilisateurs.

Sélectionnez le choix « Edit End Entity Profile », entrez un nom de profil et sélectionnez le bouton « Add Profile ». Sélectionnez ensuite le profile dans la liste et le bouton « Edit End Entity Profile ».



Ecran 7 : Profil de l'entité utilisateur final

Cet écran va permettre de définir les champs que devra remplir l'administrateur de RA, lors de l'inscription d'un utilisateur. On crée le masque de saisie de la RA.

Pour quasiment tous les champs, deux cases à cocher permettent de spécifier si le champ est obligatoire et s'il peut être modifié.

Si un champ est marqué comme non modifiable et s'il comporte plusieurs valeurs séparées par un point virgule, alors, lors de l'ajout d'un utilisateur avec ce profil, le champ apparaîtra comme une liste déroulante. L'administrateur pourra choisir une des options entrées dans le profil. Par exemple, le champ OU peut contenir les valeurs « Marketing ; Finance ». L'administrateur de RA aura le choix entre ces deux OU. Cela ne fonctionne pas, si le champ est marqué comme modifiable.

Le DN du certificat est composé de plusieurs champs. Ces champs peuvent être sélectionnés dans une liste déroulante et ajoutés au profil.

La liste des modèles de certificats est également composée ici.

Le format de génération du certificat peut être défini. Les choix possible sont « User Generated ». Dans ce cas, les clés sont générées par l'utilisateur. Si ce format est choisi, il ne peut pas y avoir de recouvrement. Les autres choix correspondent à des formats de fichiers contenant les clés et le certificat.

Un mail peut être envoyé à l'utilisateur final, pour lui signifier que sa demande de certificat est acceptée. Attention, l'adresse mail du destinataire est extraite du certificat. Il est donc obligatoire de définir le champ d'adresse mail dans le profil (Alternate Subject Name, RFC822 Name).

Le texte du message peut contenir des séquences spéciales permettant de transférer des informations sur le compte en cours de création.

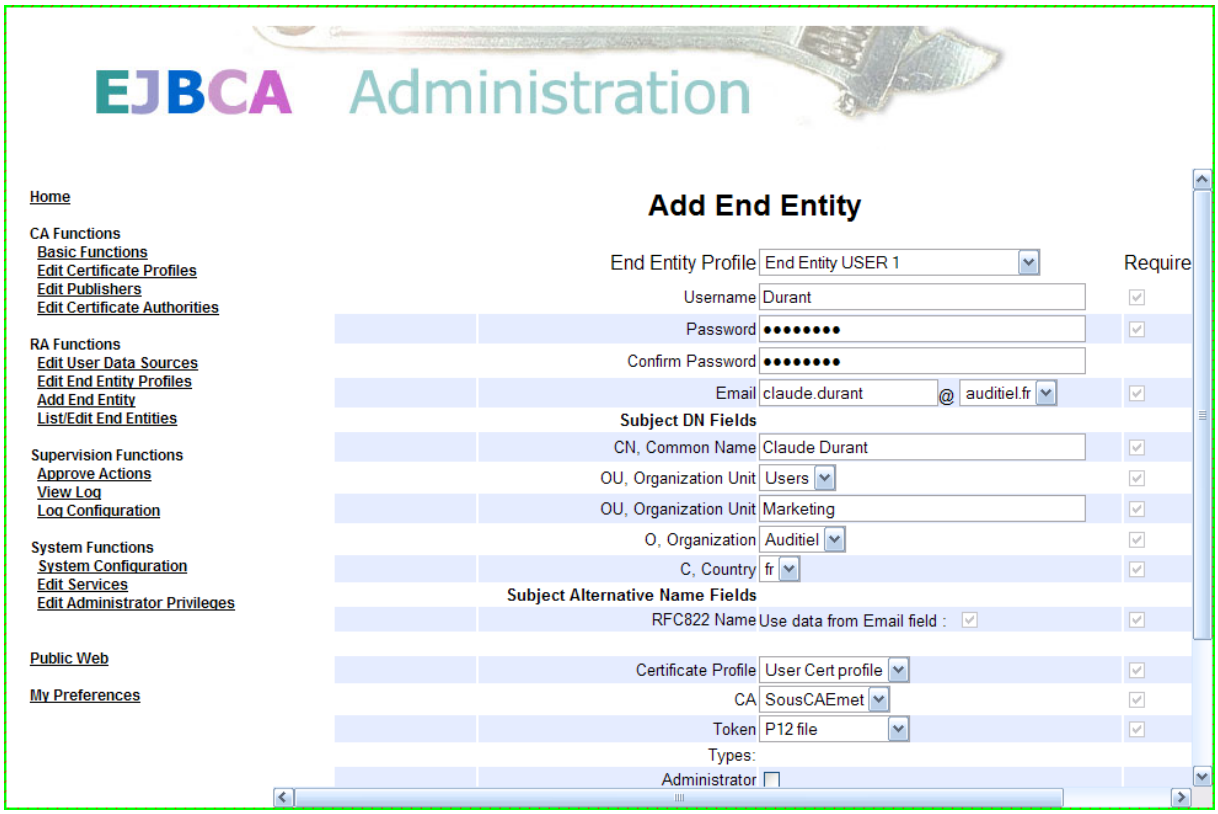
Voici un exemple de message formaté pour signifier l'autorisation de génération de certificat avec le mot de passe pour accéder au compte. Ce texte est inséré dans le champ « Notification Message ».

```
PKI interne le ${DATE}
Voici le mot de passe associé à votre demande de certificat ${NL}
Utilisateur : ${USERNAME}
Mot de passe : ${PASSWORD}
```

Remarque : Pour simplifier au maximum l'exemple, un seul profil est créé. Comme nous avons besoin de certificat d'administration et d'utilisateur, le choix « Administrator » doit être coché. Ceci permettra de générer des certificats pour les administrateurs.

5.8 Création d'un utilisateur

Sélectionnez le choix « Add End Entity », sélectionnez le profil désiré (il n'y a pas le choix dans notre exemple), puis renseignez les champs. Les champs marqués comme « Required » dans le profil apparaissent avec une case cochée.



Ecran 8 : Ajout d'un utilisateur

Entrez le nom et le mot de passe choisi pour cet utilisateur. N'oubliez pas l'adresse Email, surtout si une notification doit être envoyée à l'utilisateur.

Le champ du DN contiendra le CN saisi ainsi que les autres champs définis dans le profil et qui apparaissent à l'écran.

Dans le cas de la création d'un administrateur, la case « Administrator » doit être cochée.

Lorsque tous les champs sont complétés, sélectionnez le bouton « Add End Entity ». Si un champ obligatoire n'est pas renseigné, un message vous en avertit.

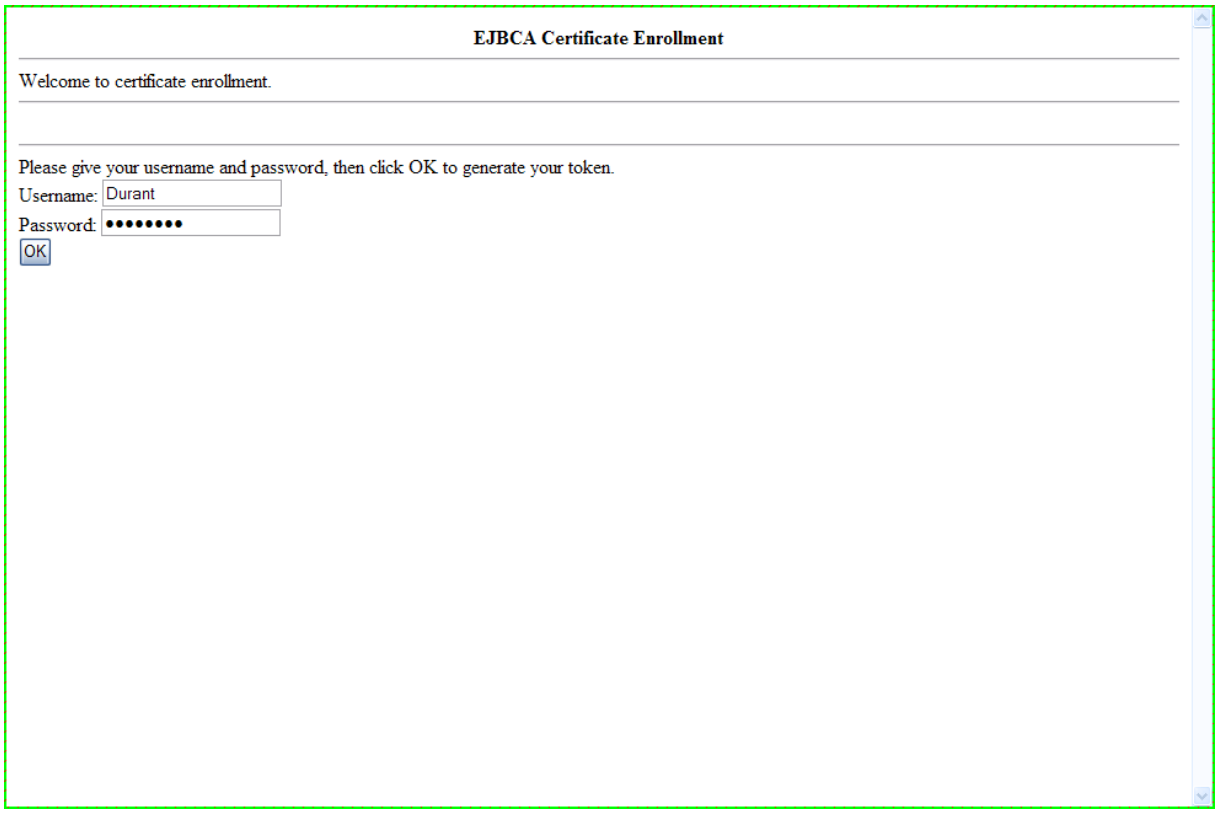
Dans le cas contraire, le formulaire s'affiche à nouveau avec un message indiquant le succès de l'opération. Le formulaire est disponible pour l'ajout d'un autre utilisateur.

5.9 Génération du certificat

Le certificat est généré lorsque l'utilisateur se connecte sur le site public d'EJBCA à l'adresse suivante :

`http://AdresseDuServeur:8080/ejbca/publicweb/apply/apply_main.jsp`

Où *AdresseDuServeur* correspond au nom DNS de la machine où est installé le serveur JBOSS.



Ecran 9 : Authentification de l'utilisateur

L'utilisateur saisit l'identifiant et le mot de passe que lui a transmis l'administrateur ou qu'il a reçus par mail.

Suivant le format de la demande l'utilisateur peut être amené à sélectionner plusieurs champs, puis il est invité à cliquer sur le bouton « OK ».

Le certificat est généré par la CA émettrice et est mis à disposition de l'utilisateur. La mise à disposition dépend du format de génération. Pour un format « User Generated », le certificat est directement inscrit dans le magasin. Dans les autres cas, le fichier est transféré sur le poste de l'utilisateur.

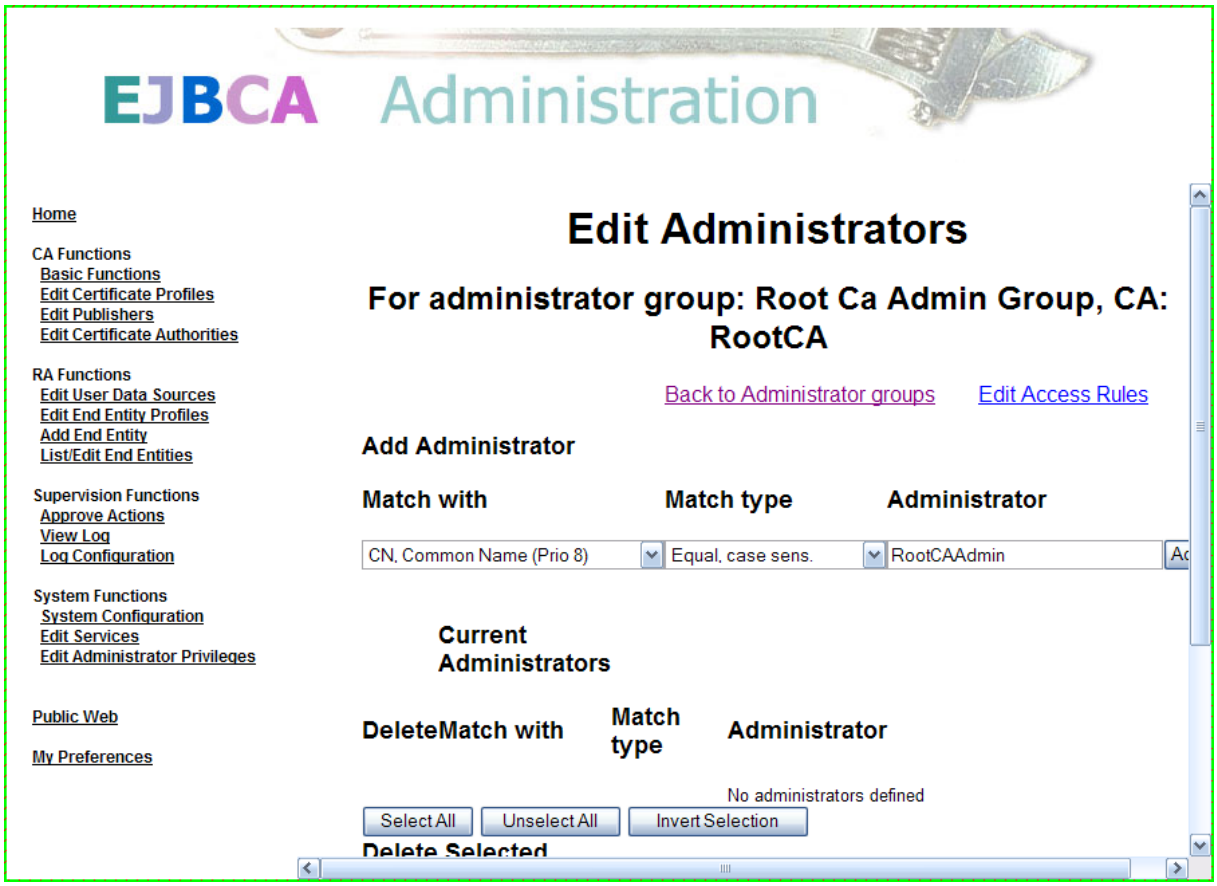
Recommencez la création d'utilisateurs finals avec les CN suivants :

- RootCAAdmin
- EmetCAAdmin
- RAAdmin

N'oubliez pas de cocher la case « Administrator » pour ces utilisateurs. Respectez la casse.

5.10 Création des groupes d'administration

Sélectionnez le choix « Edit Administrator Privileges », entrez un nouveau nom de groupe, choisissez la CA concernée puis sélectionnez le bouton « Add Administrator Group ». Sélectionnez ensuite le nouveau groupe dans la liste et sélectionnez le bouton « Edit Administrators ».



Ecran 10 : Ajout d'un administrateur dans un groupe

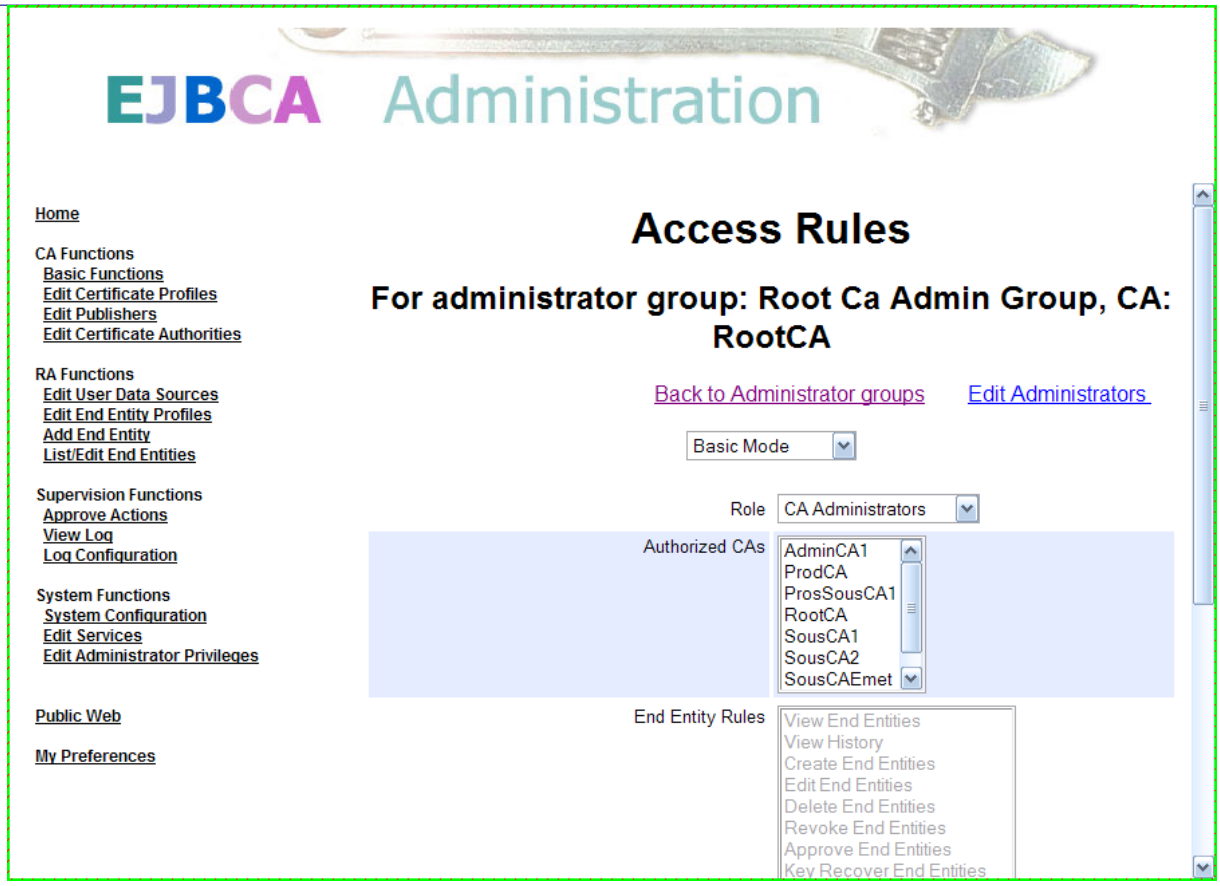
Pour reconnaître un administrateur, un champ du certificat est testé. En général, il s'agit du champ CN. Sélectionnez dans la liste « Match with » le champ désiré puis la méthode de comparaison dans « Math type » et enfin entrez la valeur de comparaison qui déterminera que le certificat présenté pour l'authentification est bien un certificat d'administrateur. Quelque soit le champ testé, le certificat doit avoir été émis avec un profil indiquant qu'il s'agit d'un certificat administrateur (case Administrator cochée).

Dans notre exemple, la comparaison est effectuée avec le cn du certificat. Attention, la casse est respectée.

Lorsque les informations sont entrées, sélectionnez le bouton « Add ».

Les noms des administrateurs sont listés dans le bas de la page.

Il faut maintenant donner des droits à ce groupe d'administrateurs. Pour cela, sélectionnez le lien « Edit Access Rules » en haut de cette page.



Ecran 11 : Rôles attribué au groupe d'administrateurs

Sélectionnez le rôle des administrateurs de ce groupe, c'est-à-dire « CA Administrators ». Puis sélectionnez les CA autorisées pour ce groupe (RootCA). Validez la saisie en sélectionnant le bouton « Save ».

Recommencez la création d'un autre groupe pour les administrateurs de la sous CA de nom SousCAEmet. Ajoutez l'administrateur EmetCAAdmin. Ce groupe aura le rôle « CA Administrators » mais uniquement de la CA de nom SousCAEmet.

Enfin, créez un dernier groupe d'administrateurs pour la RA. Le nom de l'administrateur de ce groupe est RAAdmin. Le rôle attribué à ce groupe est « RA Administrators ». Sélectionnez la CA sur laquelle le groupe d'administrateurs de la RA peut demander des certificats, c'est-à-dire SousCAEmet. Puis sélectionnez les règles sur les entités finales ainsi que les profils d'entités finales autorisés. Validez la saisie en sélectionnant le bouton « Save ».

Ecran 12 : Rôles pour un groupe d'administrateurs de RA

Lorsqu'un administrateur se connecte sur l'interface d'administration d'EJBCA, seules les fonctions autorisées sont affichées.

Ecran 13 : écran d'un administrateur de RA

La page de l'administrateur de RA est simplifiée au maximum.