

The LINAGORA logo is presented in a red, rounded rectangular box with a white background for the text. A red curved line arches over the top right of the box.

LINAGORA

The EJBCA logo features the letters 'EJBCA' in a bold, black, sans-serif font. The 'E' is enclosed in a blue square border. A small 'PKI' trademark symbol is positioned to the right of the letters.

EJBCA PKI

Groupe LINAGORA

How-To « Opérations d'administration »

EJBCA

EJBCA 3.6.1 [fr]

Version 1.0

Le 22/06/2009

Identifiant : -

Fichier original : 9999-02_DOC_EJBCA_How-To-Administration_1.0.odt

Groupe LINAGORA
27, rue de Berri
75008 PARIS
FRANCE

Tél. : +33 (0)1 58 18 68 28
Fax : +33 (0)1 58 18 68 29

<http://www.linagora.com/>

SIRET : 431 473 669 00056

Diffusion : Groupe Linagora

CC-BY-SA, GNU FDL

Réf. : 9999-02

Historique des évolutions et visas

Visas

	RÉDACTION	APPROBATION	VALIDATION
NOM	David CARELLA	Yannick QUENEC'H DU	Michel MAUDET
FONCTION	Expert PKI	Responsable du pôle Sécurité	Directeur Général Adjoint
DATE			
VISA			

Historique des évolutions

L'ajout de son nom par tout nouvel **acteur contributeur** exprime son consentement exprès et non vicié à une distribution du document conforme à la licence indiquée en page 3.

VERSION	DATE	ACTEUR CONTRIBUTEUR	OBJET DE L'ÉVOLUTION
0.1	06/06/2008	David CARELLA	Création à partir d'une extraction du guide d'administration 2.7.2
0.2	20/06/2008	David CARELLA	Mise à jour : Sigles et acronymes
0.3	02/07/2008	David CARELLA	Mise à jour : structure
1.0	22/06/2009	David CARELLA	Mise à jour : selon une version cliente finalisée

Statut du document : 60 – En application

Licence, diffusion et contributeurs

Licence

Ce document est licencié cumulativement sous licences **GNU FDL 1.3** et **CC-BY-SA 3.0**.

La **GNU FDL** est une licence libre copyleft calquée sur la GNU GPL, parfaitement adaptée aux documentations et qui nécessite que soit annexé systématiquement le texte de la licence.

La **CC-BY-SA** est une licence libre copyleft parfaitement adaptée aux contenus multimédias. Sa grande modularité permet de mixer les réalisations.

Cette double licence permet un usage du document qui soit conforme à l'une ou l'autre des licences. Plusieurs avantages peuvent être avancés :

1. Le contenu sous licence est dès lors compatible avec la totalité des licences qui lui sont adjointes ;
2. L'étendue de la double licence est limitée à celle de la licence la plus permissive ;
3. L'utilisation d'au moins une licence française sécurise la double licence au regard des dispositions françaises.

Exceptions

Par dérogation au paragraphe précédent, certaines exceptions peuvent être apportées à la cession de droits telle que consentie par la licence. Les éléments concernés par ces limitations sont les suivants :

Élément	Titre et/ou description	Licence	Remarques

Diffusion du document

Par dérogation aux paragraphes précédents, la diffusion du document est limitée de la manière qui suit :

Mention de diffusion : Groupe Linagora

NOM	ORGANISME	POUR	MÉDIA
Tous les collaborateurs	Groupe Linagora	Information	GED

Liste des contributeurs

Yannick QUENEC'HDU, Nicolas COUDÈNE, David CARELLA, André PELLÉ.

Table des matières

1	Introduction.....	8
2	How-To « Opérations d'administration ».....	10
2.1	Les AC.....	10
2.1.1	Générer une AC.....	10
2.1.2	Révoquer une AC.....	11
2.1.3	Renouveler une AC.....	11
2.1.4	Mettre en ligne ou hors ligne.....	11
2.1.5	Importer une AC.....	12
2.1.6	Exporter une AC.....	12
2.1.7	Générer une requête de certificat d'AC.....	13
2.1.8	Signer une requête externe de certificat d'AC.....	13
2.1.9	Réception d'un certificat d'AC délivré par une AC externe.....	14
2.1.10	Récupérer le certificat d'une AC.....	14
2.1.11	Obtenir des informations sur une AC.....	14
2.2	Les LCR et les delta LCR.....	15
2.2.1	Récupérer une LCR.....	15
2.2.2	Obtenir des informations sur une LCR.....	15
2.2.3	Générer une LCR.....	15
2.3	Gestion des profils de certificats.....	15
2.3.1	Créer un profil de certificats.....	15
2.3.2	Éditer un profil de certificats.....	15
2.3.3	Renommer un profil de certificats.....	16
2.3.4	Supprimer un profil de certificats.....	16
2.3.5	Utiliser un profil existant pour en générer un nouveau.....	16
2.3.6	Import/export de profil de certificats et d'entités.....	16
2.4	Service de publication.....	17
2.4.1	Créer un nouveau service de publication.....	17
2.4.2	Renommer un service de publication.....	17
2.4.3	Éditer le service de publication.....	17
2.4.4	Utiliser un service existant pour en générer un nouveau.....	18
2.4.5	Supprimer un service de publication.....	18
2.4.6	Vérification et sauvegarde du service de publication.....	18
2.4.7	Publication LDAP.....	18
2.4.8	Service de publication par script.....	22
2.5	Le menu services.....	23
2.5.1	Création d'un service de vérification d'expiration de certificats.....	23
2.5.2	Création d'un service de vérification des LCR.....	24
2.6	Recouvrement et séquestre.....	24
2.6.1	Activer le séquestre de clés dans EJBCA.....	24
2.6.2	Activer le séquestre de clés pour un profil d'entités.....	24
2.6.3	Approbation de recouvrement.....	25
2.6.4	Recouvrer une clé depuis l'interface web.....	25
2.6.5	Recouvrer une clé en ligne de commande.....	25

2.7	Gestion des requêtes.....	26
2.7.1	Paramétrage de la gestion des requêtes.....	26
2.7.2	Consultation des requêtes.....	26
2.7.3	Validation ou rejet des requêtes.....	26
2.8	Gestion de données.....	27
2.8.1	Création d'un profil de données externes.....	27
2.8.2	Édition d'un profil de données externes.....	27
2.9	Certificat.....	27
2.9.1	Requête de certificat.....	27
2.9.2	Lister et éditer des certificats.....	27
2.9.3	Consultation de certificats.....	28
2.9.4	Révocation d'un certificat.....	28
2.9.5	Impression du mot de passe.....	28
2.9.6	Notification par courriel.....	29
2.10	Les journaux.....	30
2.10.1	Consulter les journaux.....	30
2.10.2	Configuration des journaux.....	30
2.10.3	Exporter des journaux.....	30
2.10.4	Les journaux avec syslog.....	31
2.10.5	Signer les journaux.....	31
2.11	Configuration du système.....	34
2.11.1	Gestion des services.....	34
2.11.2	Gestion des administrateurs.....	36
2.12	Supervision.....	38
3	Glossaire.....	40
4	Sigles et acronymes.....	43
5	Références.....	46
6	Index.....	47

Notations

Le code informatique

Les sorties dans un **terminal** sont représentées ainsi :

```
$ commande1  
# commande2
```

Les commandes à exécuter avec des droits utilisateurs sont précédées du caractère « \$ » tandis que celles à exécuter avec les droits *root* sont précédées du caractère « # ». Ces caractères ne doivent pas être saisis dans la ligne de commandes.

Le contenu ou un extrait de **fichier** est représenté ainsi :

```
# Ceci est un exemple de fichier  
parameter1="value"  
parameter2="<NOM-DU-SERVEUR>"
```

Dans le corps de texte, les noms de variables, les extraits de code et les adresses web seront composés en police à chasse fixe. Exemples :

- l'adresse du site web de Linagora est <http://www.linagora.com/> ;
- le contenu de la variable <DATE> est de la forme JJ/MM/AAAA.

Les notes hors texte

Une **remarque** sera représentée de cette façon :

Ceci est un point sur lequel votre attention doit être attirée.

Une **alerte** sera représentée de cette façon :

Ceci est un **point critique** à prendre en compte et pour lequel votre attention est requise.

Les langues étrangères

Les **mots anglo-saxons** sont composés de deux façons : soit en caractères italiques pour les mots du langage courant ou considérés comme tels, soit en caractères droits pour les titres.

Exemples :

Voici un *English text* dans du texte français.

Le protocole Secure Socket Layer est un ...

Préambule

Ce document présente **comment faire chaque opération d'administration** pour l'interface d'administration web de l'application EJBCA. L'objectif de ce document est de présenter de manière exhaustive toutes les étapes des opérations que peut faire l'administrateur pour gérer l'IGC.

Il est conseillé que l'administrateur de l'IGC possède une culture des normes et standards sur les certificats numériques, e.g. ITU-T X.509 (certificats et LCR), protocole OCSP, codage DER.

1 Introduction

Écrit en Java/J2EE, EJBCA est une infrastructure de gestion de clés (IGC) Open Source pouvant gérer plusieurs autorités de certification (AC). Les bases du projet EJBCA sont de fournir une IGC avec un haut niveau de paramétrage comprenant les composants de bases des IGC, la gestion et la délégation des droits d'administration.

Pour réaliser à bien les opérations du cycle de vie des certificats, une IGC comprend au minimum les éléments suivants :

- une **autorité de certification** (AC) : elle est responsable de la délivrance et de la révocation des certificats ;
- une **autorité d'enregistrement** (AE) : elle vérifie le lien entre les clés publiques et les identités des titulaires (vérification de l'identité des demandeurs de certificats). L'AE est responsable des fonctions qui lui sont déléguées par l'AC, en vertu de la politique de certification ;
- une **autorité d'enregistrement locale** (AEL) : elle permet aux personnes, machines ou les agents de logiciel de demander des certificats qui pourront être employés pour signer, chiffrer, etc. ;
- un ou plusieurs **dépôts** : qui stockent et rendent disponibles les certificats et les listes des certificats révoqués (LCR) ;
- une **politique de certification** : elle définit les processus organisationnels et les informations de sécurité, ainsi que les procédés et les principes pour l'usage de la cryptographie.

Ce découpage par entités, correspond aux différents menus et fonctions que l'on retrouve dans l'IGC et que le ou les administrateurs manipuleront selon leur habilitation.

HOW-TO – Opérations d'administration

2 How-To « Opérations d'administration »

Cette section présente comment faire pas à pas toutes les opérations qu'un administrateur peut être amené à exécuter.

Pour le détail des champs, il convient de se reporter aux parties précédentes.

2.1 Les AC

2.1.1 Générer une AC

2.1.1.1 AC logiciel

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Saisir le nom de l'autorité dans le champ, puis cliquer sur le bouton « Créer ». Attention, le nom donné ici est uniquement utilisé pour identifier le certificat le certificat d'AC par EJBCA et n'a pas de rapport avec le DN de l'autorité ;
4. Sélectionner « Logiciel » dans le champ « Token du certificat de l'AC ».
5. Indiquer les informations relatives à l'AC (date d'émission des LCR, DN, politique, etc.) ;
6. Si le certificat de l'AC doit être auto-signé, choisir la valeur « Auto-signé » dans le champ « Signé par » ; dans le cas d'une AC subordonnée choisir l'AC qui émettra le certificat de cette nouvelle AC ;
7. Une fois les informations de la page saisies, cliquer sur le bouton « Créer » ;
8. La nouvelle AC a été générée.

2.1.1.2 AC matériel (hardware)

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Saisir le nom de l'autorité dans le champ, puis cliquer sur le bouton « Créer ». Attention, le nom donné ici est uniquement utilisé par EJBCA, et n'a pas de rapport avec le DN de l'autorité ;
4. Sélectionner « PKCS#11 » dans le champ « Token du certificat de l'AC ».
5. Saisir dans le champ « Propriétés du token matériel de l'AC » les informations liées à votre carte cryptographique (habituellement l'empreinte numérique de la clé), de la manière suivante :

```
defaultKey <EMPREINTE-NUMÉRIQUE>
```

6. Saisir dans le champ « Code d'authentification » le mot de passe de la clé privée générée sur la carte cryptographique ;
7. Indiquer les informations relatives à l'AC (date d'émission des LCR, DN, politique, etc.) ;
8. Si le certificat de l'AC doit être auto-signé, choisir la valeur « Auto-signé » dans le champ « Signé par », dans le cas d'une AC subordonnée choisir l'AC qui émettra le certificat de cette nouvelle AC ;

9. Une fois les informations de la page saisies, cliquer sur le bouton « Créer » ;
10. La nouvelle AC a été générée.

2.1.2 Révoquer une AC

Cette opération nécessite d'avoir préalablement tous les certificats dépendant de cette AC, ainsi que toutes référence à cette AC dans les différents profils :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Sélectionner l'AC que vous souhaitez révoquer ;
4. Appuyer sur le bouton « Éditer » ;
5. À la fin de la page, sélectionner la raison de la révocation ;
6. Cliquer sur le bouton « Révoquer » ;
7. L'AC est révoquée.

2.1.3 Renouveler une AC

Le processus de renouvellement permet de prolonger la période de validité de l'AC. ce processus permet aussi de renouveler les clés si vous souhaitez émettre de nouvelle clé pour cette AC :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Sélectionner l'AC que vous souhaitez renouveler ;
4. Cliquer sur le bouton « Éditer » ;
5. Modifier la date de l'AC ;
6. À la fin de la page, cliquer sur le bouton « Renouveler une AC » ;
7. Il est possible de renouveler les clés en cochant « Renouveler les clés » ;
8. L'AC a été renouvelée.

2.1.4 Mettre en ligne ou hors ligne

2.1.4.1 En passant par les fonctions de base

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Fonctions de base » ;
3. Rechercher, dans la page, l'AC qui doit être activée ou désactivée ;
4. Cliquer sur le lien « Informations sur l'AC » ;
5. Une fenêtre externe s'ouvre et affiche les informations sur l'AC ;
6. À la fin de cette page, au choix cliquer sur le bouton « Mettre hors ligne » pour désactiver l'AC ou saisir le mot de passe de cette AC et cliquer sur le bouton activer pour réactiver cette AC.

2.1.4.2 En passant par l'activation d'AC.

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Activation d'AC » ;
3. Rechercher, dans le tableau, l'AC qui doit être activée ou désactivée ;
4. Cocher l'action voulue dans la colonne Activer / Mettre hors ligne.
5. Il est nécessaire de compléter le champ « Code d'authentification » avec le code d'authentification qui protège le keystore contenant les AC (Default: foo123).
6. Cliquer sur « Appliquer ».
7. Le statut de l'AC apparaît dans la colonne « Statut de l'AC »

2.1.5 Importer une AC

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Cliquer sur le bouton « Importer une AC... » ;
4. Saisir les champs, de la manière suivante :
 - a. Le premier champ « Le nom que vous souhaitez donner à l'AC » est le nom qui va identifier de manière générique l'AC dans EJBCA. Ce nom n'a pas de rapport avec le DN de l'AC,
 - b. Indiquer le chemin vers le fichier PKCS#12 de l'AC à importer dans le champ « Chemin complet du fichier PKCS #12 qui contient les clés de l'AC » ,
 - c. Saisir le mot de passe du fichier PKCS#12 dans le champ « Mot de passe du keystore » ,
 - d. Optionnel : saisir un ALIAS pour la clé de signature,
 - e. Optionnel : saisir un ALIAS pour la clé de chiffrement ;
5. Cliquer sur le bouton « Importer une AC ».

Le processus d'importation est terminé, votre AC doit être à présent affichée dans la liste des « Autorités de certification ».

Remarque : il est possible à la suite de l'importation de paramétrer certaines valeurs de cette AC, telles que la période d'émission de la LCR, la période de validité de la LCR, la période de validité de cette AC, etc. Pour cela, éditer l'AC et modifier les champs souhaités.

2.1.6 Exporter une AC

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Sélectionner l'AC que vous souhaitez exporter ;
4. Cliquer sur le bouton « Éditer » ;
5. À la fin de la page d'édition, saisir dans le champ « L'exportation de l'AC nécessite un mot de passe pour l'AC » le mot de passe qui protège cette AC et pour protéger le fichier PKCS#12 d'export de l'AC ;

6. Cliquer sur le bouton « Exporter l'AC.. » ;
7. Sauvegarder le fichier PKCS #12 ;
8. Le processus d'exportation d'une AC est terminé.

Attention : EJBCA 3.4.5 exporte avec mot de passe de l'AC générique.

2.1.7 Générer une requête de certificat d'AC

Ce processus permet de générer une requête de certificat d'AC depuis EJBCA.

Remarque : préalablement à la création de la requête, il faut se munir du certificat de l'AC qui va signer cette requête de certificat. Le certificat doit être au format Base64 (PEM).

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Saisir un nom pour votre AC (ce nom n'a pas de rapport avec le DN du certificat de l'AC.) ;
4. Cliquer sur le bouton « Créer » ;
5. Indiquer les informations relatives à l'AC (date d'émission des LCR, DN, politique, etc.) ;
6. Choisir pour le champ « Signé par », la valeur « AC externe », pour indiquer que ce certificat sera émis par une AC externe à cette PKI ;
7. Une fois votre demande de requête correctement saisie, cliquer sur le bouton « Faire une requête de certificat » ;
8. Indiquer le fichier contenant l'AC qui va signer cette requête. Le fichier doit être au format Base64 (PEM) ;
9. Télécharger la requête de certificat ;
10. Le processus de requête pour une AC externe est terminé.

2.1.8 Signer une requête externe de certificat d'AC

Il faut se munir de la requête de certificat au format Base64 (PEM) au préalable.

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Saisir un nom pour la nouvelle AC (ce nom n'a pas de rapport avec le DN du certificat de l'AC.) ;
4. Cliquer sur le bouton « Processus de demande de certificat » ;
5. Indiquer le chemin de votre fichier de requête de certificat ;
6. Cliquer sur le bouton « Processus de demande de certificat » ;
7. Sélectionner l'AC signataire et saisir au minimum la date de validité du certificat ;
8. Cliquer sur le bouton « Processus de demande de certificat » ;
9. Le processus de signature d'une AC externe est terminé.

Remarque : il est possible par la suite de paramétrer certaines valeurs de cette AC, telles que la période d'émission de la LCR, la période de validité de la LCR, la période de validité de cette AC, etc. Pour se faire, éditer l'AC et modifier les champs souhaités.

2.1.9 Réception d'un certificat d'AC délivré par une AC externe

Il faut se munir du fichier contenant le certificat d'AC au format Base64 (PEM) au préalable.

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Sélectionner l'AC dont une requête de certificat a été faite : l'AC est dans l'état « En attente de réponse » ;
4. Cliquer sur le bouton « Éditer » ;
5. Cliquer sur le bouton « Réception de la réponse du certificat » ;
6. Indiquer le chemin du fichier contenant votre certificat d'AC signé ;
7. Cliquer sur le bouton « Réception de la réponse du certificat » ;
8. Le processus de réception d'une réponse de certificat d'AC est terminé.

2.1.10 Récupérer le certificat d'une AC

La récupération des certificats est possible soit par la page publique de la PKI, soit par l'intermédiaire de la page d'administration.

Pages publiques :

1. Se connecter à EJBCA sur l'interface publique ;
2. Cliquer sur « Récupérer les certificats AC et OCSP » (« *Fetch CA & OCSP Certificates* ») ;
3. Cliquer sur le certificat et le type de format souhaité.

Interface d'administration :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Fonctions de base » ;
3. Sélectionner l'AC pour laquelle vous souhaitez obtenir le certificat ;
4. Cliquer sur le lien « Télécharger pour » pour obtenir le certificat selon le format souhaité.

2.1.11 Obtenir des informations sur une AC

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Fonctions de base » ;
3. Sélectionner l'AC pour laquelle vous souhaitez obtenir des informations ;
4. Cliquer sur le lien « Visualiser les informations ».

2.2 Les LCR et les delta LCR

2.2.1 Récupérer une LCR

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Fonctions de base » ;
3. Sélectionner l'AC pour laquelle vous souhaitez obtenir la LCR ;
4. Cliquer sur le lien « Télécharger la LCR » pour obtenir la LCR.

2.2.2 Obtenir des informations sur une LCR

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Fonctions de base » ;
3. Cliquer sur le lien « Visualiser les informations » de l'AC dont vous souhaitez obtenir des informations, notamment celles sur sa LCR ;
4. Les informations sur la LCR apparaissent dans une nouvelle fenêtre.

2.2.3 Générer une LCR

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Fonctions de base » ;
3. Rechercher l'AC pour laquelle vous souhaitez générer une LCR ;
4. Cliquer sur le bouton « Créer la LCR ».

2.3 Gestion des profils de certificats

2.3.1 Créer un profil de certificats

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Saisir le nom du profil dans le champ, puis cliquer sur le bouton « Ajouter » ;
4. Le nouveau profil a été généré. Il faut maintenant éditer ses options.

2.3.2 Éditer un profil de certificats

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Sélectionner le profil que vous voulez éditer et cliquer sur « Éditer le profil d'entité » ;
4. Modifier les différentes valeurs comme la longueur de la clé, son ou ses utilisation(s), etc. ;

5. Une fois les informations de la page saisies cliquer sur le bouton « Enregistrer » ;
6. Les modifications du profil ont été prises en compte.

2.3.3 Renommer un profil de certificats

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Sélectionner le profil que vous voulez renommer ;
4. Saisir le nouveau nom du profil sélectionné ;
5. Cliquer sur « Renommer la sélection » ;
6. Le profil a été renommé.

2.3.4 Supprimer un profil de certificats

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Sélectionner le profil que vous voulez supprimer ;
4. Cliquer sur « Supprimer » ;
5. Le profil a été supprimé.

2.3.5 Utiliser un profil existant pour en générer un nouveau

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Saisir le nom du profil dans le champ ;
4. Sélectionner le profil existant que vous voulez utiliser comme modèle ;
5. Cliquer sur le bouton « Utiliser le gabarit sélectionné » ;
6. Le nouveau profil a été généré.

2.3.6 Import/export de profil de certificats et d'entités

2.3.6.1 Exporter les profils

1. Ouvrir un terminal ;
2. Se rendre dans le répertoire de EJBCA ;
3. Exécuter la commande suivante :

```
./bin/ejbca.sh ca exportprofiles <RÉPERTOIRE-DE-SAUVEGARDE>
```

4. Les profils de certificats et d'entités ont été sauvegardés au format XML dans le répertoire <RÉPERTOIRE-DE-SAUVEGARDE>.

2.3.6.2 Importer les profils

1. Ouvrir un terminal ;

2. Se rendre dans le répertoire de EJBCA ;
3. Exécuter la commande suivante :

```
./bin/ejbca.sh ca importprofiles <RÉPERTOIRE-DE-SAUVEGARDE>
```

4. Les profils de certificats et d'entités ont été importés à partir des sauvegardes au format XML du répertoire <RÉPERTOIRE-DE-SAUVEGARDE>.

2.4 Service de publication

2.4.1 Créer un nouveau service de publication

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Saisir le nom du profil dans le champ, puis cliquer sur le bouton « Ajouter » ;
4. Le nouveau service de publication a été généré. Il faut maintenant éditer ses options.

2.4.2 Renommer un service de publication

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Sélectionner le service que vous voulez renommer ;
4. Saisir le nouveau nom du service sélectionné ;
5. Cliquer sur « Renommer la sélection » ;
6. Le service de publication a été renommé.

2.4.3 Éditer le service de publication

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Sélectionner le profil que vous voulez éditer et cliquer sur « Éditer » ;
4. Modifier les différentes valeurs comme le type de serveur de publication, l'adresse du serveur, le DN de base, le nom d'utilisateur et le mot de passe d'un administrateur de ce DN, etc. ;
5. Une fois les informations de la page saisies cliquer sur le bouton « Enregistrer et tester la connexion » ;
6. Si la configuration est correcte, la connexion est établie ; sinon il faut modifier la configuration selon l'erreur et cliquer à nouveau sur « Enregistrer et tester la connexion » ;
7. Les modifications du service de publication ont été prises en compte et le test de connexion est réussi.

2.4.4 Utiliser un service existant pour en générer un nouveau

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Saisir le nom du profil dans le champ, sélectionner le service qui va servir de modèle puis cliquer sur le bouton « Utiliser le gabarit sélectionné » ;
4. Le nouveau service de publication a été généré sur le modèle d'un service existant.

2.4.5 Supprimer un service de publication

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Sélectionner le service que vous voulez supprimer ;
4. Cliquer sur « Supprimer le service de publication » ;
5. Le service de publication a été effacé.

2.4.6 Vérification et sauvegarde du service de publication

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Sélectionner le service dont il faut vérifier la connexion et cliquer sur « Éditer » ;
4. Cliquer maintenant sur « Enregistrer et tester la connexion » ;
5. Si le message suivant s'affiche, alors la connexion avec le service de publication a pu se faire donc la configuration est correcte. Sinon se reporter au message d'erreur pour corriger le problème.

Éditer un service de publication
Service de publication : Publication LDAP
Connexion testée avec succès

2.4.7 Publication LDAP

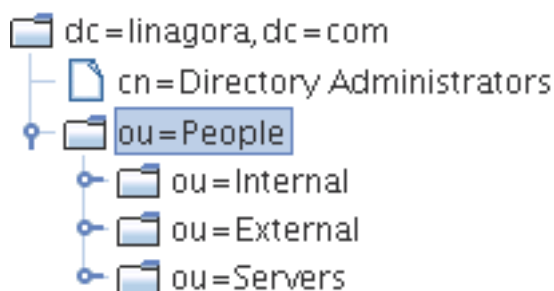
Avant tout, assurez-vous de disposer d'un serveur LDAP fonctionnel (que vous pouvez interroger avec les commandes `ldapsearch`, `ldapadd`). Les informations suivantes sont requises :

- l'adresse IP (ou nom DNS) du serveur LDAP ;
- suffixe de l'annuaire (`BaseDN`, e.g. `dc=linagora,dc=com`) ;
- un DN utilisateur disposant de droits d'écriture dans l'annuaire ;
- le mot de passe de cet utilisateur.

Il est fortement recommandé d'activer le support SSL au niveau du serveur LDAP.

2.4.7.1 Exemple d'arbre

Nous utiliserons – dans cet exemple – un DIT (Directory Information Tree) structuré de la manière suivante :



L'insertion des certificats se fera à partir de la branche « **People** », qui a pour DN `ou=People,dc=linagora,dc=com`. Les différentes OU (*Organizational Unit*) filles correspondent à des champs qui seront utilisés dans les certificats.

2.4.7.2 Préparation du serveur LDAP

2.4.7.2.1 Sun One Directory Server

Afin de segmenter les autorisations, il est recommandé de créer un utilisateur spécial pour la publication depuis EJBCA. Nous utiliserons dans cet exemple l'utilisateur :

```
cn=EJBCA,ou=Security,dc=linagora,dc=com
```

Pour autoriser cet utilisateur à modifier le serveur LDAP, il faut créer une ACI (*Access Control Instruction*) :

```
# ldapsearch -xZZ ldap://ldap.linagora.com/ -b 'dc=linagora,dc=com' -s base aci > aci.ldif
```

Ouvrir le fichier « `aci.ldif` » et rajouter l'entrée suivante :

```
aci: (targetattr ="*") (target="ldap:///ou=People,dc=linagora,dc=com") (version 3.0;
acl "EJBCA LDAP Publisher"; allow (all) userdn =
"ldap:///cn=EJBCA,ou=Security,dc=linagora,dc=com");)
```

Cette ACI donne tous les droits (lecture, écriture, modification) sur la branche :

```
OU=People,DC=linagora,DC=com
```

Pour l'utilisateur :

```
cn=EJBCA,ou=Security,dc=linagora,dc=com
```

2.4.7.3 Configuration de la publication

2.4.7.3.1 Paramètres serveur

1. Se connecter sur l'interface d'administration EJBCA ;
2. Cliquer sur le lien « Services de publication » ;
3. Définir un nom pour le service de publication (e.g. « Publication LDAP ») ;

Ajouter

Publication LDAP

4. Cliquer sur le service puis sur « Éditer le service de publication » ;
5. Choisir le type « LDAPv3 » ;
6. Remplir les champs :

- nom d'hôte,
- vérifier l'action du SSL le cas échéant (le choix du numéro de port est automatique),
- BaseDN (dans notre exemple : ou=People,dc=linagora,dc=com),
- l'identifiant (DN) de l'utilisateur LDAP (cn=EJBCA,ou=Security,dc=linagora,dc=com),
- mot de passe de l'utilisateur LDAP.

Paramètres LDAP:	
Nom d'hôte:	ldap.linagora.com
Port	636 Utiliser SSL <input checked="" type="checkbox"/>
Positionner la localisation des champs pour former un LDAP DN	DN de base ou=People,dc=linagora,dc=com
Identifiant (sous forme de DN)	EJBCA,ou=Security,dc=linagora,dc=com
Mot de passe	*****
Confirmer mot de passe	*****

2.4.7.3.2 objectClass et attributs

Les champs Classe d'objets utilisateur, Classe d'objets de l'AC permettent de définir les object-Class qui seront utilisés pour la publication respective d'un certificat utilisateur et d'un certificat d'AC. Les champs suivants permettent de définir les noms des attributs LDAP qui seront utilisés pour la publication du contenu :

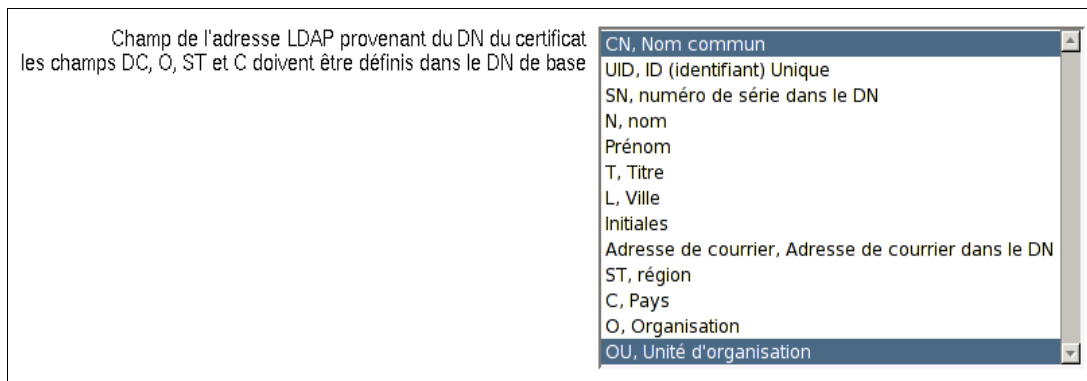
- attribut du certificat utilisateur (**userCertificate**) ;
- attribut du certificat d'AC (**cACertificate**) ;
- attribut de la LCR (**certificateRevocationList**) ;
- attribut de la LAR (**authorityRevocationList**).

Il est recommandé de **ne pas modifier** ces valeurs qui correspondent aux valeurs standards.

Classe d'objets utilisateur	top;person;organizationalPerso
Classe d'objets de l'AC	top;applicationProcess;certifica
Attribut de certificat utilisateur	userCertificate;binary
Attribut de certificat d'AC	cACertificate;binary
Attribut de LCR	certificateRevocationList;binary
Attribut de delta LCR:	deltaRevocationList;binary
Attribut de LAR (liste des autorités révoquées)	authorityRevocationList;binary

2.4.7.3.3 Correspondance des champs du certificat vers LDAP

Choisir dans ce champ les attributs du certificat qui seront utilisés pour la construction du DN LDAP. Par exemple :



2.4.7.4 Vérification et sauvegarde du profil de publication

Cliquer sur le bouton « Sauvegarder et tester la connexion », si le paramétrage est correct, vous devez obtenir le message suivant :



2.4.7.5 Activation de la publication LDAP

2.4.7.5.1 Définir le service de publication d'un profil de certificats

La publication se configure au niveau des profils de certificats.

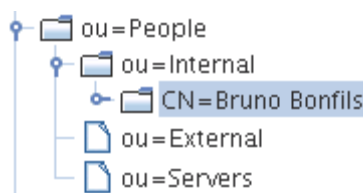


2.4.7.5.2 Publication d'un certificat déjà présent

Dès l'activation de la publication, tous les certificats générés utilisant ce profil de certificats seront publiés dans l'annuaire LDAP. Notez qu'il est également possible de publier à nouveau un certificat déjà généré. Pour ce faire, vous devez utiliser l'interface Lister/Éditer les certificats. Une fois le certificat trouvé, cliquer sur « Voir certificats » puis sur le bouton « Republier ».

2.4.7.6 Vérification de la publication

Une fois le premier certificat publié, il est recommandé de vérifier que sa publication est effective.



Attribute	Value
userCertificate;binary	BINARY (814b)
ou	Internal
givenName	Bruno
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	inetOrgPerson
sn	Bonfils
o	Linagora
cn	Bruno Bonfils

Certificate Info
Subject: CN=Bruno Bonfils, OU=Internal, O=Linagora, C=FR
Issuer: OU=Internal, DC=linagora, DC=com
Validity From: Tue Oct 03 10:23:25 CEST 2006
To: Thu Oct 02 10:33:25 CEST 2008
Sig. Algorithm: SHA1withRSA Serial Number: 6523164527389207608 Version: 3

Ces captures d'écrans sont issues du logiciel libre LBE (LDAP Browser Explorer) [LBE] qui permet la navigation et l'édition d'un annuaire LDAP, avec le support des certificats (authentification, lecture, écriture).

2.4.8 Service de publication par script

Depuis la version 3.6, il est possible de faire la publication à l'aide de scripts lisibles par la machine exécutant EJBCA. Ainsi un script Bash, Perl, Ruby, etc. pourra se charger de la publication.

Pour cela, il faut créer et éditer un service de publication comme vu précédemment :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Services de publication » ;
3. Saisir le nom du profil dans le champ, puis cliquer sur le bouton « Ajouter » ;
4. Le nouveau service de publication a été généré. Il faut maintenant éditer ses options ;
5. Sélectionner le profil que vous venez de créer et appuyer sur « Éditer » ;
6. Sélectionner « Service de publication personnalisé » comme type de service ;
7. Saisir « `org.ejbcacore.model.ca.publisher.GeneralPurposeCustomPublisher` » pour le chemin de classe ;
8. Pour les propriétés de paramétrage du service de publication plusieurs choix sont possibles :

```
crl.application /fullpathname/exportscript.sh
crl.failOnStandardError <true | false>
crl.failOnErrorCode <true | false>
cert.application /fullpathname/exportscript.sh
cert.failOnStandardError <true | false>
cert.failOnErrorCode <true | false>
revoke.application /fullpathname/exportscript.sh
revoke.failOnStandardError <true | false>
revoke.failOnErrorCode <true | false>
```

Des variables existent pour différents types d'événements :

- a. Les variables « `cr1.*` » à la création d'une nouvelle LCR,

- b. Les variables « `cert.*` » à la création d'un nouveau certificat,
- c. Les variables « `revoke.*` » à la révocation d'un certificat.

Les types de variables sont les mêmes pour les trois types d'événements :

- a. Les variables de type « `*.application` » contiennent le chemin absolu du script qui sera exécuté,
- b. Les variables de type « `*.failOnStandardError` » permettent l'envoi des types d'erreur à la console lorsqu'elles sont positionnées à « `true` »,
- c. Les variables de type « `*.failOnErrorCode` » permettent l'envoi des codes d'erreur EJBCA par le script lorsqu'elles sont positionnées à « `true` ».

Pour exécuter les scripts, des paramètres doivent être passés en argument selon les événements :

- a. Le paramètre « `crl.application` » prend un argument : la nouvelle LCR au format DER,
- b. Le paramètre « `cert.application` » prend deux arguments : 1. Le fichier du nouveau certificat, 2. Le type de ce certificat,
- c. Le paramètre « `revoke.application` » prend deux arguments : 1. Le fichier de révocation et le deuxième la raison.

Voici un exemple de script Bash pour exporter la LCR lorsqu'elle a été mise à jour dans un répertoire d'un serveur web (le paramètre « `$1` » reçoit la valeur du premier argument du script, ici la nouvelle LCR) :

```
#!/bin/sh
cp $1 /var/www/crl/plop.crl
```

- 9. Une fois les informations de la page saisies, cliquer sur le bouton « Sauvegarder et tester la connexion » ;
- 10. Si la configuration est correcte, la connexion est établie. Sinon il faut modifier la configuration en fonction de l'erreur et cliquer à nouveau sur « Sauvegarder et tester la connexion » ;
- 11. Les modifications du service de publication ont été générées et le test de la connexion est réalisé.

2.5 Le menu services

2.5.1 Création d'un service de vérification d'expiration de certificats

- 1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions système ;
- 2. Cliquer sur le lien « Créer/Éditer services » ;
- 3. Saisir le nom du service dans le champ ;
- 4. Cliquer sur le bouton « Créer » ;
- 5. Sélectionner le service créé ;
- 6. Cliquer sur le bouton « Éditer » ;
- 7. Sélectionner « Vérificateur d'expiration de certificats » pour le travail du service ;

8. Modifier les différentes valeurs : les AC à vérifier, l'intervalle de vérification et les options de notifications ;
9. Ne pas oublier de cocher la variable « Actif » pour activer le service ;
10. Cliquer sur « Sauvegarder » ;
11. Le nouveau service de vérification d'expiration de certificats a été créé.

2.5.2 Création d'un service de vérification des LCR

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions système ;
2. Cliquer sur le lien « Créer/Éditer services » ;
3. Saisir le nom du service dans le champ ;
4. Cliquer sur le bouton « Créer » ;
5. Sélectionner le service à créer ;
6. Cliquer sur le bouton « Éditer » ;
7. Sélectionner « Vérificateur des LCR » pour le travail du service ;
8. Modifier les différentes valeurs : l'intervalle de vérification ;
9. Ne pas oublier de cocher la case « Actif » pour activer le service ;
10. Cliquer sur « Sauvegarder » ;
11. Le nouveau service de vérification des LCR a été créé.

2.6 Recouvrement et séquestre

Pour être en mesure de recouvrer une clé privée associée à un certificat, la fonctionnalité doit être activée dans la configuration d'EJBCA. Le recouvrement de clés est généralement utilisé pour des certificats utilisés pour du chiffrement (de document notamment), en effet si la clé privée associée à un certificat utilisé pour chiffrer des documents est perdue, les documents chiffrés ne seront plus déchiffrables. C'est pourquoi EJBCA fournit un système permettant le stockage et le recouvrement des clés privées.

2.6.1 Activer le séquestre de clés dans EJBCA

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Configuration du système » ;
3. Cocher l'option « Activer le recouvrement de clés » ;
4. Cliquer sur le bouton « Suivant » puis « Enregistrer » ;
5. Le séquestre de clés a été activé.

2.6.2 Activer le séquestre de clés pour un profil d'entités

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Éditer les profils d'entités » ;

3. Sélectionner le profil pour lequel vous voulez activer le séquestre de clés ;
4. Cliquer sur « Éditer » ;
5. Cocher l'option « Clé recouvrable », le cas échéant vous pouvez aussi cocher les options « Par défaut » ou « Requis » ;
6. Cliquer sur le bouton « Sauvegarder » ;
7. Le séquestre de clés pour le profil choisi a été activé.

2.6.3 Approbation de recouvrement

Cf. § 2.7.3 Validation ou rejet des requêtes, page 26.

2.6.4 Recouvrer une clé depuis l'interface web

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Lister/Éditer les entités » ;
3. Sélectionner les informations à l'entité que vous voulez recouvrer ;
4. Cliquer sur « Lister » ;
5. Dans la liste des entités, cliquer cette fois sur « Éditer l'entité » ;
6. Sélectionner « Nouveau » dans l'état du certificat et rentrer un mot de passe ;
7. Cliquer sur le lien « Interface publique », puis « Créer un certificat client » ;
8. Taper le nom et le mot de passe de l'entité à recouvrer ;
9. Choisir la longueur de la clé et valider ;
10. La clé a été recouvrée.

2.6.5 Recouvrer une clé en ligne de commande

1. Se munir du nom de l'entité, du numéro de série du certificat en hexadécimal et du nom de l'émetteur au format DN (ex. : CN=AdminCA1,O=EJBCA Sample,C=SE) que l'on veut recouvrer ;
2. Ouvrir un terminal ;
3. Exécuter les commandes suivantes :

```
# cd $EJBCA_HOME
# ./bin/ejbca.sh ra revokeuser <NOM-UTILISATEUR> 0
# ./bin/ejbca.sh ra keyrecovertnewest <NOM-UTILISATEUR>
# ./bin/ejbca.sh ra setclearpwd <NOM-UTILISATEUR> <NOUVEAU-MOT-DE-PASSE>
# ./bin/ejbca.sh batch
```

4. Le recouvrement a été effectué.

Attention : si l'interface ligne de commande est utilisée, le certificat de l'administrateur n'étant pas utilisé pour cette opération, il pourra lui-même procéder à l'approbation via l'interface web.

2.7 Gestion des requêtes

2.7.1 Paramétrage de la gestion des requêtes

2.7.1.1 Activation des notifications par courriel des approbations

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions systèmes ;
2. Cliquer sur le lien « Configuration du système » ;
3. Cocher « Activer la notification des approbations » ;
4. Rentrer un alias courriel pointant vers les adresses courriels des administrateurs ;
5. Rentrer l'adresse courriel de l'expéditeur des courriels ;
6. Cliquer sur « Suivant » puis « Sauvegarder » ;
7. La notification par courriel des approbations a été ajoutée.

2.7.1.2 Activation des approbations dans une AC

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Éditer/créer les AC » ;
3. Sélectionner l'AC à laquelle il faut ajouter des approbations ;
4. Cliquer sur « Éditer » ;
5. Sélectionner les actions à approuver sur la ligne « Paramètres d'approbation » ;
Les actions peuvent être l'ajout et la suppression d'une entité, la révocation des certificats et le recouvrement de clés ;
6. Sélectionner le nombre d'approbations nécessaire ;
7. Cliquer sur « Sauvegarder » ;
8. Les approbations ont été activées.

2.7.2 Consultation des requêtes

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions de supervision ;
2. Cliquer sur le lien « Gestion des requêtes » ;
3. Sélectionner les requêtes à voir en fonction de leur statut : exécuté, approuvé, rejeté, en attente, toutes, ... ;
4. Cliquer sur « Lister » ;
5. Les actions ont été listées.

2.7.3 Validation ou rejet des requêtes

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions de supervision ;
2. Cliquer sur le lien « Gestion des requêtes » ;
3. Cliquer sur l'action qu'il faut valider ou rejeter ;

4. Optionnel : Rentrer un commentaire ;
5. Cliquer sur « Valider » pour approuver ou « Rejeter » pour rejeter l'action ;
6. L'action a été validée ou non, selon le choix fait.

2.8 Gestion de données

Il est nécessaire au préalable de créer un profil de données externes selon les spécifications en vigueur.

2.8.1 Création d'un profil de données externes

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité AE ;
2. Cliquer sur le lien « Gestion des données externes » ;
3. Saisir le nom du profil dans le champ ;
4. Cliquer sur le bouton « Ajouter » ;
5. Le profil a été créé ; il faut maintenant l'éditer.

2.8.2 Édition d'un profil de données externes

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité AE ;
2. Cliquer sur le lien « Gestion des données externes » ;
3. Sélectionner le profil à éditer puis cliquer sur « Éditer les données externes » ;
4. Remplir tous les champs sans oublier le champ « Chemin de classe » qui est le chemin java pour accéder à la définition du profil de données ;
5. Cliquer sur le bouton « Enregistrer et tester la connexion » pour tester si le paramétrage ;
6. Le profil a été édité.

2.9 Certificat

2.9.1 Requête de certificat

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Ajouter une demande d'entité » ;
3. Sélectionner le profil d'entités que l'on souhaite pour ce certificat ;
4. Remplir et sélectionner les champs nécessaires : mot de passe, nom, autorité de certification, type de certificats, *token*, etc. ;
5. Cliquer sur « Ajouter une demande d'entité » ;
6. La création d'une requête pour un certificat a été créée.

2.9.2 Lister et éditer des certificats

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;

2. Cliquer sur le lien « Lister/Éditer les entités » ;
3. Sélectionner le mode avancé ou normal pour rechercher les certificats ;
4. Remplir les champs nécessaires à la recherche ;
5. Cliquer sur « Lister » ;
6. La liste des certificats associés à votre recherche a été créée ;
7. Pour éditer un certificat, cliquer sur « Éditer entité ».

2.9.3 Consultation de certificats

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Lister/Éditer les entités » ;
3. Sélectionner le mode avancé ou normal pour consulter le ou les certificats concernés ;
4. Remplir les champs nécessaires à la recherche ;
5. Cliquer sur « Lister » ;
6. Pour voir les détails d'une entité, cliquer sur « Voir entité » ;
7. Pour voir le certificat généré de l'entité, cliquer sur « Voir certificat » ;
8. Pour voir l'historique des opérations sur cette entité, cliquer sur « Voir historique ».

2.9.4 Révocation d'un certificat

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Lister/Éditer les entités » ;
3. Sélectionner le mode avancé ou normal pour rechercher le certificat à révoquer ;
4. Remplir les champs nécessaires à la recherche ;
5. Cliquer sur « Lister » ;
6. Cliquer sur « Voir certificat » sur la ligne de l'entité au certificat à révoquer ;
7. Sélectionner le certificat voulu dans le cas où il en existe plusieurs en appuyant sur « Voir le suivant » ;
8. Sélectionner la raison de révocation ;
9. Cliquer sur « Révoquer » ;
10. Le certificat a été révoqué.

2.9.5 Impression du mot de passe

2.9.5.1 Activation de l'impression dans un profil d'entités

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Sélectionner le profil pour lequel il faut ajouter l'impression de mot de passe ;
4. Cliquer sur « Éditer le profil d'entité » ;

5. Cocher l'option « Utiliser » sur la ligne « Impression des données de l'entité » ;
6. Sélectionner une imprimante et le format d'impression, et rentrer le nombre de copies souhaitées ;
7. Cliquer sur « Enregistrer ».

2.9.5.2 Activation de l'impression dans une entité

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Ajouter une demande d'entité » ;
3. Sélectionner le profil avec impression ;
4. Cochez l'option d'impression « Imprimer les données de l'entité » et cocher les autres options « Par défaut » et « Requis » le cas échéant ;
5. Remplir les autres champs ;
6. Cliquer sur « Ajouter une demande d'entité » ;
7. L'impression des données de l'entité et donc de son mot de passe a été effectuée.

2.9.6 Notification par courriel

2.9.6.1 Activation de la notification dans un profil d'entités

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;
3. Sélectionner le profil pour lequel il faut ajouter la notification par courriel ;
4. Cliquer sur « Éditer le profil d'entités » ;
5. Cocher l'option « Utiliser » sur la ligne « Notification par courriel » et cocher les autres options « Par défaut » et « Requis » le cas échéant ;
6. Remplir les champs associés : adresse de l'expéditeur, le titre et le corps du courriel ;
7. Cliquer sur « Enregistrer ».

2.9.6.2 Activation de la notification dans une entité

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Ajouter une demande d'entité » ;
3. Sélectionner le profil avec notification ;
4. Remplir les champs adresse courriel de l'entité ;
5. Cochez l'option « Notifier l'utilisateur » ;
6. Remplir les autres champs ;
7. Cliquer sur « Ajouter une demande d'entité » ;
8. L'entité a été prévenue par courriel de la requête pour un certificat.

2.10 Les journaux

2.10.1 Consulter les journaux

Il existe deux modes pour consulter les journaux : un simple qui ne permet de voir les événements sans distinction sur leur type, l'autre avancé qui permet de voir des événements associés à des AC, des certificats, etc. ou encore des types d'événements et bien sûr de sélectionner un intervalle de temps :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions de supervision ;
2. Cliquer sur le lien « Consulter les journaux » ;
3. Choisir le type de consultation Simple ou Avancé ;
4. Choisir la période de temps en mode Simple où remplir les champs suivants en mode Avancé a été choisi ;
5. Valider en appuyant sur le bouton « Voir » ;
6. Pour rafraîchir la liste cliquer sur « Recharger » ;
7. Le journal des événements associés aux paramètres a été généré.

2.10.2 Configuration des journaux

Pour chaque AC, il est possible de choisir les événements de type information ou erreur qui seront enregistrés dans les journaux, on peut aussi décider de n'avoir que des journaux internes (stockés dans une base de données locale) ou bien externes (stockés sur un autre serveur) ou encore les deux :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions de supervision ainsi que les droits d'accès à l'entité d'AC ;
2. Cliquer sur le lien « Configuration des journaux » ;
3. Sélectionner l'AC pour laquelle il faut configurer les journaux ;
4. Cliquer sur le bouton « Sélectionner » ;
5. Sélectionner les événements qui doivent être enregistrés et si l'on souhaite utiliser des journaux internes, externes ou les deux ;
6. Cliquer sur « Enregistrer » ;
7. Les journaux associés à une AC ont été configurés.

2.10.3 Exporter des journaux

Il est possible d'exporter les journaux au format CSV, ensuite importable dans un logiciel de tableur par exemple. On peut aussi signer les journaux exportés avec une AC, ce qui peut être utile lorsque l'on souhaite authentifier la provenance et garantir l'intégrité des journaux :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions de supervision ;
2. Cliquer sur le lien « Consulter les journaux » ;
3. Choisir le type de consultation « Mode de Base » ou « Mode Avancé » ;
4. Choisir le délai en mode Simple ou remplir les champs suivants en Mode Avancé ;

5. Valider en appuyant sur le bouton « Voir » ;
6. Facultatif : sélectionner l'AC avec laquelle il faut signer les journaux ;
7. Cliquer sur « Exporter au format CSV » ;
8. Votre navigateur télécharge un fichier « `logexport.csv` » contenant la liste des événements ;
9. Les événements sélectionnés ont été exportés.

2.10.4 Les journaux avec syslog

Il est possible d'enregistrer les journaux via un serveur syslog qu'il soit local ou distant. Pour cela, il faut modifier la configuration du serveur JBoss et relancer le démon syslog pour que ce dernier accepte des connexions si ce n'était pas déjà le cas.

Remarque : en procédant de cette manière, ni la recompilation de EJBCA ni la relance du serveur JBoss n'est nécessaire.

Il convient de procéder de cette manière :

1. Ouvrir une console dans le répertoire `$HOME_JBOSS/server/default/conf` ;
2. Éditer le fichier `jboss-log4j.xml` et à la fin ajouter ceci en l'adaptant. Par exemple en paramétrant la valeur « `SyslogHost` » (adresse du serveur syslog) et le niveau de log :

```
[...]

<appender name="SYSLOG" class="org.apache.log4j.net.SyslogAppender">
  <errorHandler class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
  <param name="Facility" value="local7"/>
  <param name="FacilityPrinting" value="true"/>
  <!-- Adresse du serveur syslog -->
  <param name="SyslogHost" value="localhost"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="[%d{ABSOLUTE}],%c{1}] %m%n"/>
  </layout>
</appender>

<category name="org.ejbca">
  <!-- Niveau de log : INFO, WARN, DEBUG -->
  <priority value="DEBUG"/>
  <appender-ref ref="SYSLOG"/>
</category>

[...]
```

3. Ajouter à la fin du fichier de configuration du serveur syslog `/etc/syslog.conf` :

```
local7.* /var/log/ejbca.log
```

4. Vérifier que le serveur syslog est lancé avec l'option « `-r` », si ce n'est pas le cas, le relancer avec cette option en plus ;
5. Les journaux sont maintenant enregistrés par un serveur syslog dans le fichier :
`/var/log/ejbca.log`

2.10.5 Signer les journaux

Les journaux contiennent des informations qui peuvent se révéler critiques comme les certificats créés et révoqués, etc. À partir de la version 3.6 de EJBCA, il est possible de signer toutes

les entrées des journaux. Ainsi comme chaque entrée représente un événement, chaque événement sera répertorié et haché à l'aide d'une fonction de hachage (SHA-1 ou SHA-256) permettant de détecter toute altération des journaux. Un attaquant ne pourra pas passer inaperçu en effaçant ses actions dans les journaux, chaque entrée manquante ou altérée faisant remonter une erreur de comparaison des empreintes des événements enregistrés.

Pour activer la signature des journaux, il convient de suivre la procédure suivante :

1. Arrêter JBoss ;
2. Aller dans le répertoire `$HOME_EJBCA/conf` ;
3. Dupliquer le fichier `log.properties.samples` en `log.properties` ;
4. Ouvrir ce dernier et ajouter la ligne suivante :

```
usedLogDevices=Log4jLogDevice;ProtectedLogDevice
```

5. La variable `usedLogDevices` représente la liste des systèmes de journaux utilisés. Les systèmes sont définis plus bas dans le fichier. Le système `Log4jLogDevice` est celui par défaut géré par JBoss. La syntaxe pour ajouter un système de journaux est :

```
NomDuSystemeDeJournaux=LaClasseDuSysteme;LeFichierDeConfiguration
```

Le fichier de configuration est optionnel.

6. Dans le répertoire `logdevices`, dupliquer le fichier `protectedlog.properties.sample` en `protectedlog.properties` ;
7. Ce fichier contient toute la configuration de la protection des journaux. Pour l'explication de toutes les variables, se reporter au tableau ci-après. Il faut au minimum paramétrer les variables suivantes :

`protectionTokenReferenceType` et `protectionTokenReference` ;

8. Compiler et déployer EJBCA à nouveau :

```
$ ant clean
$ ant deploy
```

9. Relancer le serveur JBoss ;
10. Si c'est la première fois que les journaux signés sont activés il convient d'accepter la configuration en exécutant la commande suivante :

```
$ cd $EJBCA_HOME
$ ./bin/ejbca.sh log accept conf/logdevices/protectedlog.properties
```

Vous devez alors taper un nombre pour vérifier que vous voulez bien valider la configuration. Ensuite si tout a bien fonctionné, le résultat de cette commande est :

```
Signing...
SUCCESS!
```

11. Les journaux sont maintenant signés.

Variables du fichier `$EJBCA_HOME/logdevices/protectedlog.properties` :

Variable	Description
<code>protectionTokenReference</code>	Token utilisé pour la signature des journaux. Il est possible d'utiliser un fichier JKS contenant le certificat de signature dans ce cas on met l'adresse menant au JKS. Ou bien alors on se sert d'une AC de EJBCA dans ce cas on met le nom de l'AC.
<code>protectionTokenReferenceType</code>	Type de token pour la signature des journaux. Si on utilise une AC de EJBCA, il faut mettre « CAName ». Si on utilise un JKS il faut mettre

	« URI ». Si on rentre « none » aucun token ne sera utilisé pour la signature.
<code>protectionTokenKeyStoreAlias</code>	Si on utilise un JKS, il convient de mettre l'alias du JKS.
<code>protectionTokenKeyStorePassword</code>	Si on utilise un JKS, il convient de renseigner son mot de passe.
<code>protectionIntensity</code>	Intervalle de temps en minutes entre chaque signature. « 0 » veut dire qu'on signe chaque événement/entrée.
<code>protectionHashAlgorithm</code>	Fonction de hachage utilisée pour chaîner les journaux exportés : SHA-1 ou SHA-256.
<code>allowConfigurableEvents</code>	Par défaut la signature des journaux journalise tous les événements quelle que soit la configuration réalisée dans l'interface d'administration. Si cette option est positionnée à « TRUE » alors la signature des journaux prend en compte la configuration définie dans l'interface d'administration. Ce n'est pas conseillé parce qu'un attaquant pourrait de cette manière désactiver toute journalisation.
<code>verificationService.active</code>	À « TRUE » cela permet d'activer la vérification des journaux.
<code>verificationService.invokationinterval</code>	Intervalle de temps en minutes entre deux vérifications des journaux.
<code>verificationService.freezeThreshold</code>	Temps au-delà duquel, si aucune entrée n'a été inscrite dans les journaux, les journaux sont considérés gelés.
<code>exportService.active</code>	Il existe un service pour exporter les journaux de la base de données
<code>exportService.invokationinterval</code>	Intervalle de temps en minutes entre deux exportations de journaux.
<code>exportService.deleteAfterExport</code>	Positionner à « TRUE » permet d'effacer les journaux une fois exportés.
<code>exportService.exportOlderThan</code>	Si on veut effacer les journaux après les avoir exportés, il faut convenir d'une date au-delà de laquelle les journaux seront exportés. Cette variable est exprimée en minutes.
<code>exportService.exportHandler</code>	Classe Java qui gère l'exportation des journaux. Par défaut deux classes sont disponibles : <ul style="list-style-type: none"> - <code>org.ejbca.core.model.log.ProtectedLogDummyExportHandler</code> qui exporte sur la sortie standard de la console : - <code>org.ejbca.core.model.log.ProtectedLogCMSExportHandler</code> exporte au format CMS, enveloppe de données signée au format PKCS #7.
<code>cmsexport.caname</code>	Dans le cas d'une exportation au format CMS, il convient de spécifier l'AC dans EJBCA qui va signé.
<code>cmsexport.fullpath</code>	Dans le cas d'une exportation au format CMS, il convient de spécifier le chemin absolu du répertoire dans lequel on souhaite trouver les journaux exportés.
<code>useMailAction</code>	Il est possible d'envoyer un courriel dans le cas d'une compromission des journaux. Pour activer ce service, il faut positionner cette variable sur « TRUE »
<code>mailAction.senderAddress</code>	Adresse à laquelle envoyer le courriel.

<code>mailAction.emailAddresses</code>	Si plusieurs adresses utilisez cette variable en séparant les adresses par des points virgules.
<code>mailAction.subject</code>	Sujet du courriel.
<code>mailAction.body</code>	Corps du courriel.
<code>useScriptAction</code>	Il est possible de lancer des scripts exécutables en local. Pour activer cette fonction, il faut positionner cette variable à « TRUE ».
<code>scriptAction.target</code>	Chemin vers le script à lancer.

2.11 Configuration du système

2.11.1 Gestion des services

Il existe trois types de services pré-existants, la gestion de LCR, la notification d'expiration des certificats et l'expiration du mot de passe utilisateur. Si l'on souhaite avoir d'autres services il est nécessaire de l'écrire en langage Java et de spécifier le répertoire dans lequel se trouve le programme java contenant le service.

2.11.1.1 Ajouter un service

Si on souhaite ajouter un service personnalisé c'est-à-dire n'étant pas un des deux services pré-existant, il convient de concevoir un programme java de ce service :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions systèmes ;
2. Cliquer sur le lien « Gestion des services » ;
3. Remplir le champ « Ajouter » avec le nom du service à ajouter ;
4. Cliquer sur « Ajouter » ;
5. Un service a été ajouté, il convient maintenant de le modifier, cf. section « Modifier un service ».

2.11.1.2 Renommer un service

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions systèmes ;
2. Cliquer sur le lien « Éditer les services » ;
3. Sélectionner le service à renommer ;
4. Remplir le champ « Ajouter » avec le nouveau nom du service ;
5. Cliquer sur « Renommer le service sélectionné » ;
6. Le service a été renommé.

2.11.1.3 Modifier un service

La valeur « Chemin de classe pour l'action » correspond à l'endroit où se trouve le programme Java qui contient le service que l'on souhaite ajouter :

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions systèmes ;

2. Cliquer sur le lien « Gestion des services » ;
3. Sélectionner le service à modifier ;
4. Cliquer sur « Modifier » ;
5. Remplir et sélectionner les valeurs qu'il vous faut pour votre service ;
6. Sélectionner un service pré-existant et remplir les valeurs de notifications courriel ;
ou
indiquer le répertoire d'accès du programme Java de votre service. Remplir les valeurs associées à ce programme et remplir les valeurs de notifications courriel ;
7. Ne pas oublier de cocher la case « Actif » pour activer le service ;
8. Cliquer sur « Enregistrer » ;
9. Le service a été modifié.

2.11.1.4 Supprimer un service

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions systèmes ;
2. Cliquer sur le lien « Gestion des services » ;
3. Sélectionner le service à supprimer ;
4. Cliquer sur « Supprimer le service » ;
5. Le service a été supprimé.

2.11.1.5 Les services existants

Actuellement, il existe trois types de services prédéfinis :

- vérification de validité de la LCR (et recréation de celle-ci le cas échéant) ;
- notification par courrier électronique de l'expiration de certificats.
- expiration du mot de passe utilisateur.

Il est également possible d'appeler sa propre classe en sélectionnant le type.

2.11.1.5.1 Gestion de LCR

Ce service permet de vérifier que toutes les LCR générées sont valides, si l'une d'entre elles n'est pas valide, le service procédera à son renouvellement :

1. Cliquer sur le menu « Gestion des services » ;
2. Saisir le nom du service (p. ex. « Vérification des LCR ») ;
3. Sélectionner le service et cliquer sur « Modifier » ;
4. Choisir « Mise à jour de la LCR » comme choix de l'action ;
5. Choisir l'intervalle entre deux vérifications ;
6. Cocher le bouton « Actif » ;
7. Cliquer sur le bouton « Enregistrer » ;
8. Le service de gestion de LCR a été créé.

2.11.1.5.2 Notification d'expiration de certificats

La notification d'expiration de certificats peut être envoyée indépendamment au porteur du certificat (en utilisant l'adresse de courrier fourni à la création de celui-ci) et/ou à l'administrateur (via une adresse fournie lors de la configuration du service) :

1. Cliquer sur le menu « Gestion des services » ;
2. Saisir le nom du service (p. ex. « Notification d'expiration (1 mois) ») ;
3. Cliquer sur le bouton « Ajouter » ;
4. Sélectionner le service préalablement créé puis cliquer sur le bouton « Modifier » ;
5. Choisir « Vérification d'expiration de certificats » pour le choix de l'action ;
6. Sélectionner les AC à surveiller ;
7. Choisir le délai avant expiration, pour chaque certificat expirant dans le délai donné, une notification sera émise ;
8. Pour chaque destinataire (porteur du certificat, administrateur), définir le sujet du courrier ainsi que le corps du message. Pour le corps du message, les variables $\{CN\}$, $\{O\}$, $\{OU\}$ du sujet du certificat peuvent être utilisées.

2.11.1.5.3 Service d'expiration du mot de passe

Le service d'expiration du mot de passe vérifie si un utilisateur a généré un certificat au cours d'un délais définit (demande d'entité à l'état « Nouveau »). Passé ce délais si l'utilisateur n'a pas généré le certificat le statut de la demande d'entité passe à l'état « généré », l'utilisateur ne sera plus en mesure de générer le certificat.

1. Cliquer sur le menu « Gestion des services » ;
2. Saisir le nom du service (p. ex. « Expiration du mot de passe (1 mois) ») ;
3. Cliquer sur le bouton « Ajouter » ;
4. Sélectionner le service préalablement créé puis cliquer sur le bouton « Modifier » ;
5. Choisir « Service d'expiration du mot de passe » pour le choix de l'action ;
6. Sélectionner les AC à surveiller ;
7. Choisir le délai avant expiration. Pour chaque mot de passe expirant dans le délai donné, une notification peut être émise à destination de l'utilisateur et/ou de l'administrateur en cochant la case correspondante ;
8. Pour chaque destinataire (porteur du certificat, administrateur), définir le sujet du courrier ainsi que le corps du message. Pour le corps du message, les variables $\{CN\}$, $\{O\}$, $\{OU\}$ du sujet du certificat peuvent être utilisées.

2.11.2 Gestion des administrateurs

Il est possible de créer des groupes d'administrateurs aux privilèges différents pour bien cloisonner les différentes actions possibles dans EJBCA.

2.11.2.1 Création d'un compte d'administrateur

2.11.2.1.1 Activation de la création d'entité d'administration dans un profil d'entités

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Gestion des profils d'entités » ;

3. Sélectionner le profil pour lequel il faut ajouter la possibilité de création d'entité d'administration ;
4. Cliquer sur « Éditer le profil d'entités » ;
5. Cocher l'option « Utiliser » au niveau du champ « Administrateur » et cocher les autres options « Par défaut » et « Requis » le cas échéant ;
6. Cliquer sur « Enregistrer ».

2.11.2.1.2 Création d'une entité d'administration

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès à l'entité d'AE ;
2. Cliquer sur le lien « Ajouter une demande entité » ;
3. Sélectionner le profil d'entités qui a l'attribut « Administrateur » activé ;
4. Cocher l'option « Administrateur » et sélectionner « Fichier p12 » dans la ligne « Token » ;
5. Remplir et sélectionner les autres champs nécessaires : mot de passe, nom, autorité de certification, type de certificat, etc. ;
6. Cliquer sur « Ajouter une demande entité » ;
7. La création d'une requête pour un certificat administrateur a été créée.

L'administrateur n'a plus qu'à récupérer ses clés et son certificat au format PKCS #12 (fichier d'extension « p12 »).

2.11.2.1.3 Ajout de l'entité dans un groupe d'administrateurs

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions système ;
2. Cliquer sur le lien « Gestion des administrateurs » ;
3. Sélectionner le groupe d'administrateurs dans lequel il faut ajouter l'entité ;
4. Cliquer sur « Éditer le groupe » ;
5. Sélectionner l'attribut qui identifie l'entité – par exemple son CN – et saisir la valeur de cet attribut – par exemple superadmin2 ;
6. Cliquer sur « Ajouter » ;
7. Une nouvelle règle a été ajoutée permettant d'identifier le certificat et de lui appliquer les droits défini pour ce groupe.

La règle apparaît en bas de la liste. Si l'administrateur recherché n'existe pas, un lien apparaît sur l'identifiant utilisé (ex. : `superadmin2`), il convient alors de le créer à l'aide d'une demande d'entité ou d'ajouter la règle avec le bon identifiant et de supprimer l'erreur (cf. paragraphe suivant).

2.11.2.2 Suppression d'un compte d'administrateur

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions système ;
2. Cliquer sur le lien « Gestion des administrateurs » ;
3. Sélectionner le groupe d'administrateurs dans lequel il faut supprimer le compte d'administrateur ;
4. Cliquer sur « Éditer le groupe » ;

5. Sélectionner dans la liste des administrateurs ceux qu'il faut supprimer en cochant la case dans la colonne « Supprimer » ;
6. Cliquer sur « Supprimer » ;
7. Le ou les comptes d'administrateur ont été supprimés.

2.11.2.3 Création et édition des privilèges administrateur

Il est possible de créer des groupes d'administrateurs. Chaque groupe définit un ensemble de privilèges et est associé à une AC ayant servi à signer les certificats pour lesquels on se propose de donner les droits d'administrateurs. Deux modes d'édition des privilèges existent : le mode normal et le mode avancé. Dans le mode avancé, on peut définir toutes les actions possibles. Tandis que, dans le mode normal, on définit des groupes d'actions le plus souvent associés à un type d'administration (AC, AE, superviseur, super-administrateur).

2.11.2.4 Création d'un groupe d'administrateurs

1. Se connecter à EJBCA en tant qu'administrateur possédant les droits d'accès aux fonctions système ;
2. Cliquer sur le lien « Gestion des administrateurs » ;
3. Rentrer le nom du groupe qu'il faut créer, par exemple : Admin AC ;
4. Sélectionner sur quelle AC est associé le groupe ;
5. Cliquer sur « Ajouter un groupe d'administrateurs » ;
6. Sélectionner le groupe ainsi créé ;
7. Cliquer sur « Éditer les droits d'accès » ;
8. Sélectionner le mode de modification des privilèges, par exemple « Mode de base » ;
9. Choisir les privilèges, par exemple on sélectionne « Administrateur des AC » comme « Rôle » et « Toutes » pour les AC autorisées ;
10. Cliquer sur « Enregistrer » ;
11. Un nouveau groupe d'administrateur a été créé.

2.11.2.5 Édition d'un groupe d'administrateurs

1. Se connecter à EJBCA en tant qu'administrateur qui possède les droits d'accès aux fonctions système ;
2. Cliquer sur le lien « Gestion des administrateurs » ;
3. Sélectionner le groupe à modifier ;
4. Cliquer sur « Éditer les droits d'accès » ;
5. Sélectionner le mode de modification des privilèges : « Normal » ou « Avancé » ;
6. Sélectionner les valeurs en conséquence ;
7. Cliquer sur « Enregistrer » ;
8. Un nouveau groupe d'administrateur a été édité.

2.12 Supervision

Un script de supervision est disponible pour vérifier le bon fonctionnement de EJBCA. Afin de s'assurer de la continuité du service, il est possible de l'exécuter régulièrement. Ce script inclut

la gestion de *traps* SNMP pour avoir une meilleure gestion des erreurs. Le script `check-ejbca.sh` se trouve dans le répertoire `$EJBCA_HOME/supervision/`. Le fichier `LINAGORA-MIB.txt` contient la base de données des *traps* SNMP utilisée par le script de supervision. Il est possible de l'ajouter au niveau de l'agent SNMP, ceci de manière optionnelle.

Avant d'utiliser le script, il est nécessaire de le paramétrer. Pour cela, il faut l'ouvrir et adapter les paramètres suivants :

Paramètre	Description
<code>EJBCA_HOME</code>	Répertoire d'installation de EJBCA
<code>EJBCA_SH</code>	Répertoire des fichiers exécutables de EJBCA (optionnel)
<code>TODAY</code>	Date courante pour la création de l'utilisateur (optionnel)
<code>USER_DN</code>	DN de l'utilisateur (optionnel)
<code>USER_NAME</code>	Nom de l'utilisateur (optionnel)
<code>USER_PASSWORD</code>	Mot de passe de l'utilisateur (optionnel)
<code>CA_NAME</code>	AC émettrice du certificat de l'utilisateur
<code>TOKEN</code>	Type de <i>token</i> pour le certificat : P12, JKS, PEM, BROWSEGEN
<code>CERT_PROFILE</code>	Profil de certificats utilisé pour le certificat de l'utilisateur (optionnel)
<code>ENTITY_PROFILE</code>	Profil d'utilisateurs utilisé (optionnel)
<code>LOG_FILE</code>	Journal des événements du script (optionnel)
<code>ERROR_FILE</code>	Journal des erreurs du scripts (optionnel)
<code>OID_PREFIX</code>	Préfixe de l'identifiant de la MIB des <i>traps</i> du script (optionnel)
<code>SNMP_MANAGER</code>	Adresse de l'agent SNMP chargé d'envoyer les messages
<code>SNMP_COMMUNITY</code>	Réseau SNMP utilisé
<code>CRL_FILE</code>	Emplacement de sauvegarde la LCR récupérée par le script (optionnel)

3 Glossaire

Autorité de certification (AC)	<p>L'AC est responsable des certificats signés en son nom et de l'ensemble de l'infrastructure à clé publique qu'elle a mise en place. En particulier, l'AC assure les fonctions suivantes :</p> <ul style="list-style-type: none">- mise en application de la politique de certification (PC) ;- émission des certificats ;- gestion des certificats ;- publication de la liste des certificats révoqués (LCR) ;- journalisation et archivage des événements et informations relatives au fonctionnement de l'IGC. <p>L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.</p>
Liste des certificats révoqués (LCR)	<p>Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation. Cette liste est signée par l'AC émettrice.</p>
OID (<i>object identifier</i>)	<p>Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO et ITU pour désigner un objet ou une classe d'objets spécifiques. Les OID officiels sont gérés par l'IANA (Internet Assigned Numbers Authority).</p>
OCSP (Online Certificate Status Protocol)	<p>OCSP est un protocole défini dans le RFC 2560. Le but d'OCSP est de surmonter les limitations imposées par les LCR de base et de fournir une réponse immédiate et à jour aux questions sur le statut d'un certificat donné. Une information spécifique de révocation pour un certificat est retournée plutôt qu'une grande liste linéaire de recherche sous forme de LCR.</p>
Autorité d'enregistrement (AE)	<p>L'AE est responsable des fonctions qui lui sont déléguées par l'AC, en vertu de la politique de certification.</p> <p>L'AE assure habituellement les fonctions suivantes :</p> <ul style="list-style-type: none">- gestion des demandes de certificats ;- vérification de l'identité des demandeurs de certificats ;- archivage des dossiers de demandes de certificats ;- vérification des demandes de révocation de certificats.
Infrastructure de gestion des clés (IGC)	<p>Également appelée « infrastructure à clé publique » (ICP), une PKI (public key infrastructure) est un ensemble de technologies, organisations, procédures et pratiques qui supporte l'implémentation et l'exploitation de certificats basés sur la cryptographie à clés publiques.</p>
Politique de certification (PC)	<p>Ensemble de règles définissant les exigences auxquelles l'autorité de certification se conforme dans la mise en place de prestations adaptées à certains types d'applications. La politique de certification doit être identifiée de façon unique par un OID défini par l'autorité de certification.</p>
Renouvellement d'un certificat	<p>Opération effectuée à la demande d'un porteur de certificat ou en fin de période de validité d'un certificat et qui consiste à générer une nouvelle clé et émettre un nouveau certificat.</p>

Révocation d'un certificat	<p>Opération demandée par le porteur de certificat ou le responsable habilité de la société cliente, par une AC, une AE, et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité.</p> <p>La demande peut être la conséquence de différents types d'événements tels que la compromission d'une clé, le changement d'informations contenues dans un certificat, etc.</p> <p>L'opération de révocation est considérée terminée quand le certificat mis en cause est publié dans la liste des certificats révoqués.</p>
Certificat	<p>Clé publique d'un porteur de certificat, ainsi que des informations d'identité rendues infalsifiables par la signature numérique de l'autorité de certification qui l'a délivré.</p> <p>Un certificat contient des informations telles que :</p> <ul style="list-style-type: none">- l'identité du porteur de certificat ;- le numéro de série du certificat, unique par AC ;- la clé publique du porteur de certificat ;- les dates de début et de fin de vie du certificat ;- l'identité de l'autorité de certification qui l'a émis ;- la signature de l'autorité de certification qui l'a émis.
UTF-8	<p>Format de codage des caractères de l'Unicode. Le format UTF-8 est un codage à taille variable (de 1 à 4 octets par caractère) et assurant une compatibilité complète pour tous les caractères du code ASCII (7 bits). Par opposition, l'UTF-16 est un codage fixe sur 2 octets (16 bits).</p>
Autorité de certification (AC)	<p>L'AC est responsable des certificats signés en son nom et de l'ensemble de l'infrastructure à clé publique qu'elle a mise en place. En particulier, l'AC assure les fonctions suivantes :</p> <ul style="list-style-type: none">- mise en application de la politique de certification (PC) ;- émission des certificats ;- gestion des certificats ;- publication de la liste des certificats révoqués (LCR) ;- journalisation et archivage des événements et informations relatives au fonctionnement de l'IGC. <p>L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.</p>
Liste des certificats révoqués (LCR)	<p>Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation. Cette liste est signée par l'AC émettrice.</p>
OID (<i>object identifier</i>)	<p>Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO et ITU pour désigner un objet ou une classe d'objets spécifiques. Les OID officiels sont gérés par l'IANA (Internet Assigned Numbers Authority).</p>
OCSP (Online Certificate Status Protocol)	<p>OCSP est un protocole défini dans le RFC 2560. Le but d'OCSP est de surmonter les limitations imposées par les LCR de base et de fournir une réponse immédiate et à jour aux questions sur le statut d'un certificat donné. Une information spécifique de révocation</p>

pour un certificat est retournée plutôt qu'une grande liste linéaire de recherche sous forme de LCR.

4 Sigles et acronymes

Sigle	Désignation
AC	Autorité de certification
ACI	Access Control Instruction
AE	Autorité d'enregistrement
AEL	Autorité d'enregistrement locale
ARL	Authority Revocation List
ASCII	American Standard Code for Information Interchange
BER	Basic Encoding Rules
CA	Certificate Authority
CMP	Certificate Management Protocol
CMS	Cryptographic Message Syntax
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CQ	Certificat qualifié
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
CSR	Certificate Signing Request
CSV	Comma Separated Value
CVC	Card Verification Code
CVV	Card Verification Value
DB	Database
DC	Domain Component
DER	Distinguished Encoding Rules
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des pratiques de certification
EAR	Enterprise Archive
ECDSA	Elliptic Curve Digital Signature Algorithm
eID	Electronic Identity (Card)
EJB	Enterprise JavaBeans
EJBCA	EJB Certificate Authority
ETSI	European Telecommunications Standards Institute
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over SSL
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICP	Infrastructure à clé publique [fr-CA]
ID	Identifiant [en], Identifiant [fr]

Sigle	Désignation
IETF	Internet Engineering Task Force
IGC	Infrastructure de gestion de clés [fr-FR]
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
J2EE	Java 2 Enterprise Edition
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JDK	J2SE Development Kit
JKS	Java Key Store
JNDI	Java Naming and Directory Interface
JSF	Java Server Faces
JSP	Java Server Page
LAR	Liste des autorités révoquées
LBE	LDAP Browser Explorer
LCR	Liste des certificats révoqués
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LDIF	LDAP Data Interchange Format
MD5	Message Digest 5
MGF1	Mask Generation Function 1
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PC	Politique de certification
PDC	Primary Domain Controller (Microsoft Windows NT Server)
PEM	Privacy Enhancement for Internet Electronic Mail
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure [en-US], [en]
PKIX	Public Key Infrastructure for X.509 certificates
PUK	Personal Unblocking Key
QC	Qualified Certificate
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman (algorithme asymétrique)
SCEP	Simple Certificate Enrollment Protocol
SHA-1	Secure Hash Algorithm One
SHA-256	Secure Hash Algorithm 256
SP	Service de publication
SQL	Structured Query Language

Sigle	Désignation
SSL	Secure Socket Layer protocol
SVG	Scalable Vector Graphics
TCP	Transmission Control Protocol
TLS	Transport Layer Security protocol
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format
XKMS	XML Key Management Specification
XML	Extensible Markup Language

5 Références

Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE OU IDENTIFIANT
EJBCA:ADMIN	3.0	EJBCA	Guide d'administration

Références externes

RÉFÉRENCE	VER.	ÉDITEUR	TITRE OU IDENTIFIANT

Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB
EJBCA:FR	EJBCA-FR, PKI Open Source	fr-FR	http://ejbca-fr.org/
EJBCA:EN	EJBCA - The J2EE Certificate Authority - Welcome	en-US	http://www.ejbca.org/
EJBCA:MANUAL	EJBCA - User Guide	en-US	http://www.ejbca.org/manual.html
LBE	LDAP Browser Explorer	en-US	http://www.mcs.anl.gov/~gawor/ldap

6 Index

A

AC.....	8, 10, 12, 14, 40, 41
AC externe.....	14
ACI.....	19
activation.....	
approbations dans une AC.....	26
impression.....	28, 29
notification.....	29
notifications par courriel.....	26
administrateur.....	
création.....	36
gestion.....	36
AE.....	8, 40
AEL.....	8
approbation.....	26
attribut.....	20
authorityRevocationList.....	20
autorité.....	
d'enregistrement.....	8, 40
d'enregistrement locale.....	8
de certification.....	8, 40, 41

C

cACertificate.....	20
cert.application.....	23
certificat.....	
How-To.....	27
profil.....	15
requête.....	27
révocation.....	28, 41
certificat d'une AC.....	14
certificateRevocationList.....	20
configuration.....	
journaux.....	30
publication.....	19
consultation.....	
certificat.....	27, 28
des requêtes.....	26
journaux.....	30
création.....	
compte d'administrateur.....	36
profil de certificats.....	15
profil de données externes.....	27
service de publication.....	17
crl.application.....	23

D

defaultKey.....	10
delta LCR.....	15
dépôt.....	8
DIT.....	18
duplication.....	
profils de certificats.....	16

E

en ligne.....	11
expiration de certificats.....	23
exportation.....	
journaux.....	30
profil d'entités.....	16
profil de certificats.....	16

F

failOnErrorCode.....	23
failOnStandardError.....	23

G

gestion.....	
de données.....	27
des administrateurs.....	36
des requêtes.....	26
des services.....	34

H

hors ligne.....	11
How-To.....	
certificat.....	27
configuration du système.....	34
gestion de données.....	27
journaux.....	30
profils de certificats.....	15
service de publication.....	17
services.....	23

I

IGC.....	40
importation.....	
profil d'entités.....	16
profil de certificats.....	16
impression (du mot de passe).....	28

J

journaux.....	
configuration.....	30
consultation.....	30
exportation.....	30
signature.....	31

L

LAR.....	20
LCR.....	15, 20, 24, 40, 41
LDAP.....	18
ligne de commande.....	
recouvrement.....	25
log.properties.....	32

M

modification.....	
certificat.....	27
profil de certificats.....	15, 16
profil de données externes.....	27
service de publication.....	17, 18
mot de passe.....	28

N

notification.....	26
-------------------	----

O

objectClass.....	20
OCSP.....	40, 41
OID.....	40, 41

P

PC.....	40
---------	----

politique de certification.....	8	services.....	
profil.....		gestion.....	34
de données externes.....	27	SHA-1, SHA-256.....	32
protectedlog.properties.....	32	signature.....	
protectionTokenReference.....	32	journaux.....	31
protectionTokenReferenceType.....	32	Sun One Directory Server.....	19
publication.....	18, 19, 22	supervision.....	38
publication LDAP.....	21	suppression.....	
		profil de certificats.....	16
R		service de publication.....	18
recouvrement.....	24, 25	syslog.....	31
rejet (d'une requête).....	26	système (configuration).....	34
renouvellement.....	11		
requête de certificat.....	27	U	
requête de certificat d'AC.....	13	userCertificate.....	20
révocation.....	11, 28	UTF-8.....	41
revoke.application.....	23		
		V	
S		validation (d'une requête).....	26
script.....	22	vérification.....	
séquestre.....	24	expiration de certificats.....	23
séquestre de clés.....	24	LCR.....	24
serveur LDAP.....	19	service de publication.....	18