



# Guide d'installation d'un netHSM

**EJBCA**

EJBCA 3.6 [fr]

Version 1.5

Le 08/07/2008

Nom du fichier : 9999-02\_DOC\_EJBCA\_Guide-Installation-NetHSM\_1.5

## Historique des évolutions et visas

### Visas

	RÉDACTION	APPROBATION	VALIDATION
<b>NOM</b>	David CARELLA	Bruno BONFILS	Yannick QUENEC'H DU
<b>FONCTION</b>	Expert PKI	Responsable technique	Responsable du pôle Sécurité
<b>DATE</b>			
<b>VISA</b>			

### 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
1.0	19/09/2006	Bruno BONFILS	Version initiale.
1.1	26/02/2007	David CARELLA	Relecture.
1.2	27/02/2007	Yannick QUENEC'H DU	Prise en compte de la recette de pré-production.
1.3	19/04/2007	Bruno BONFILS	Corrections, ajout des sections relatives à Solaris.
1.4	13/06/2008	David CARELLA	Refonte complète du document et corrections.
1.5	08/07/2008	David CARELLA	Validation.

État du document : **60 – En application**

## Licence, diffusion et contributeurs

### Licence

Ce document est licencié cumulativement sous licences **GNU FDL 1.2** 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.

### Limitations

Par dérogation au paragraphe précédent, certaines limitations 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	Remarque

### 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

Bruno BONFILS, David CARELLA, Yannick QUENEC'H DU.

## Table des matières

<b>1</b>	<b>Introduction.....</b>	<b>7</b>
<b>2</b>	<b>Préparation de l'environnement.....</b>	<b>8</b>
2.1	Pré-requis.....	8
2.2	GNU/Linux.....	8
2.2.1	Installation des outils netHSM sous GNU/Linux.....	9
2.2.2	Installation des outils netHSM sous Solaris.....	9
<b>3</b>	<b>Paramétrage initial.....</b>	<b>10</b>
3.1	Installation du service nfast.....	10
3.2	Récupération du ESN (Electronic Serial Number) et du Keyhash.....	11
3.3	Paramétrage du RFS (Remote File System).....	11
3.4	Définition du royaume de sécurité : création des cartes administrateur. 11	
3.4.1	Utilisation du boîtier.....	11
3.5	Création des cartes opérateurs.....	12
3.5.1	Utilisation de l'outil en ligne de commande.....	13
3.6	Configuration d'un client.....	13
3.7	Vérification du bon fonctionnement.....	13
3.7.1	Création d'une clé de test.....	13
<b>4</b>	<b>Redémarrage des serveurs.....</b>	<b>15</b>
4.1	Serveur RFS.....	15
4.2	Périphérique netHSM.....	15
4.3	Redémarrage du serveur applicatif.....	16
4.3.1	Vérification de la communication entre les pilotes et le module HSM.....	16
4.3.2	Activation des AC.....	16
<b>5</b>	<b>Utilisation du netHSM pour EJBCA.....</b>	<b>17</b>
5.1	Activation du service netHSM sur le serveur RFS.....	17
5.2	Compilation d'EJBCA.....	17
<b>6</b>	<b>Création d'une clé pour génération d'un certificat racine.....</b>	<b>18</b>
6.1	Création de la clé racine.....	18
6.1.1	Présentation de l'utilitaire de génération de clés.....	18
6.1.2	Utilisation du script « keytoolncipher.sh » pour créer la clé.....	19
6.2	Création du certificat dans EJBCA.....	20
6.2.1	Modification du script de démarrage de RedHat.....	20
6.2.2	Création du certificat.....	20
<b>7</b>	<b>Suppression d'un royaume de sécurité.....</b>	<b>22</b>
<b>8</b>	<b>Références documentaires.....</b>	<b>23</b>

## 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 sont pas à saisir 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 ...

## Avertissements

**Attention :** ce document n'a pour but que de fournir une présentation rapide des modules de sécurité matériels (HSM, *Hardware Security Module*) de nCipher pour une utilisation spécifique avec l'application EJBCA. **Dans aucun cas, la lecture de ce document peut remplacer la lecture complète des documents fournis avec le module netHSM.**

**La suppression d'un royaume de sécurité doit être obligatoirement précédé de la suppression des cartes opérateurs via le boîtier netHSM.** Si cette manipulation n'est pas effectuée, il ne sera pas possible de réutiliser les cartes opérateurs.

## 1 Introduction

Ce document est un **guide d'installation** pour les modules de sécurité matériels (HSM, *Hardware Security Module*) **nethSM de nCipher** pour une utilisation spécifique avec l'application EJBCA dans les environnements **Linux RedHat** et **Solaris**.

## 2 Préparation de l'environnement

Ce document part du principe que le périphérique netHSM est connecté au réseau et est opérationnel (*i.e.* le ping est ok). Le schéma suivant décrit de manière synthétique les différentes étapes du processus d'installation du netHSM avec EJBCA.

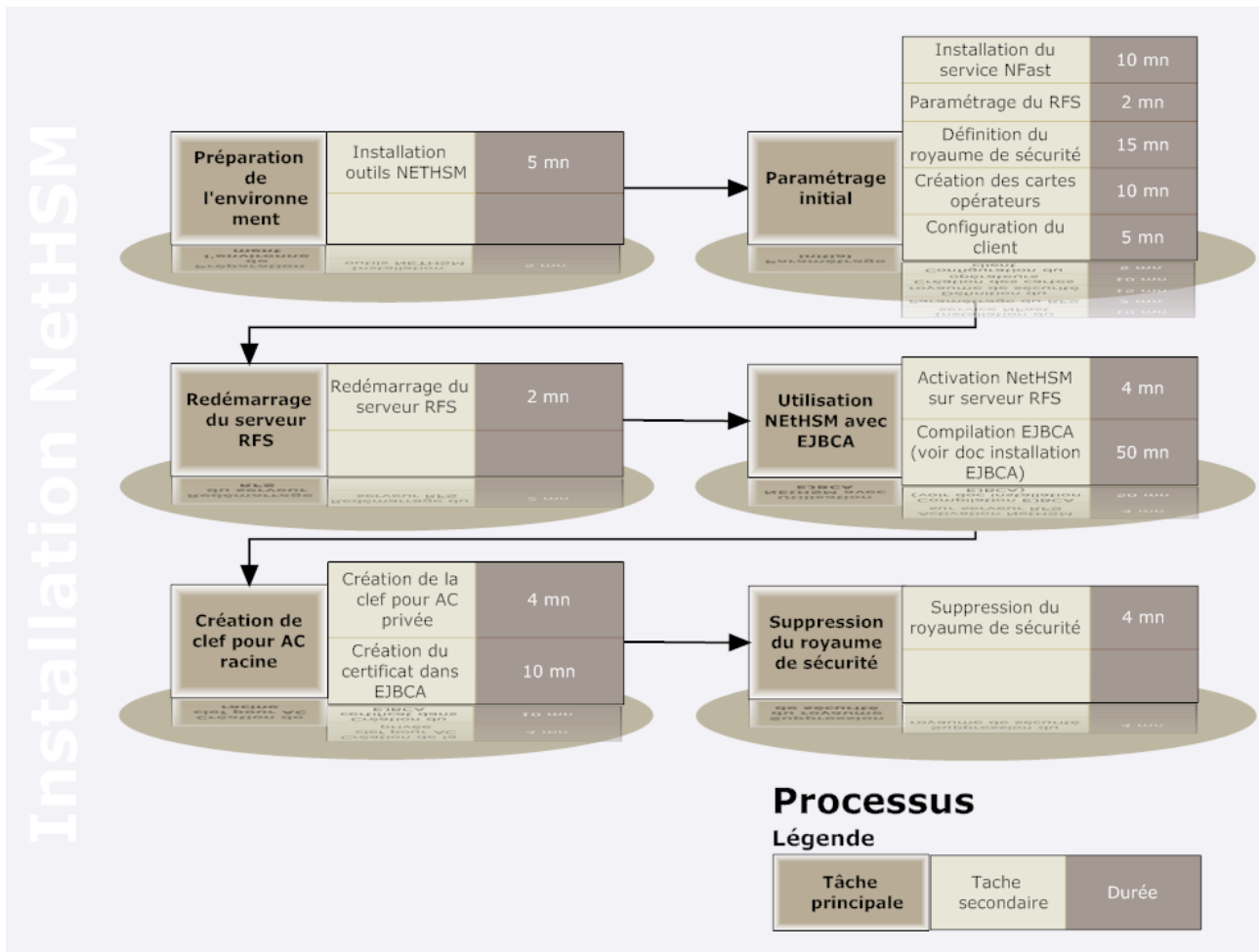


Illustration 2.1: Workflow d'installation du netHSM

### 2.1 Pré-requis

Un système d'exploitation supporté par netHSM : Solaris (x86 ou Sparc), GNU/Linux.

### 2.2 GNU/Linux

Environnements de test :

- Linux Debian Unstable (nom de code sid), 2.6.17 ;
- RedHat Enterprise 4 64 bits (Intel Xeon), 2.6.9 ;
- netHSM appliance.

### 2.2.1 Installation des outils netHSM sous GNU/Linux

1. Se connecter avec le compte `root` ;
2. Faire « `cd /tmp` » ;
3. Décompresser le fichier « `nCSS-linux-user-10.XX.tar.bz2` » ;  

```
tar xvfj nCSS-linux-user-10.XX.tar.bz2
```
4. Faire « `cd / ; for file in $(find /tmp/nCSS-linux-user-10.<XX>.tar.bz2/linux/libc6_3/nfast/ -name *.tar) ; do tar xvf $file ; done` » ;
5. Vérifiez la présence des outils dans « `/opt/nfast` ».

### 2.2.2 Installation des outils netHSM sous Solaris

1. Se connecter sur le serveur avec l'utilisateur `root` ;
2. Se déplacer dans le répertoire de montage du CD-ROM fourni par nCipher ;
3. Installer le paquetage se trouvant dans le répertoire `<RACINE-DU-CD-ROM>/solaris/2_10/amd64/nfast` à l'aide de la commande suivante :

```
pkgadd -d nfast.pkg all
```

Il est également nécessaire de définir la variable d'environnement `NFKM_LOG` qui est utilisée par certaines applications des utilitaires netHSM, c'est le cas par exemple de la commande `preload` qui permet de charger un royaume de sécurité avec un quorum supérieur à 1 pour les applications qui ne sont pas capables de gérer le changement de cartes.

Pour cela, il est recommandé de rajouter les deux lignes suivantes dans le fichier `/etc/profile` :

```
NFKM_LOG=/opt/nfast/log/nfkm.log
export NFKM_LOG
```

Puis de procéder à la création de ce fichier en définissant des droits permettant aux membres du groupe `nfast` d'écrire dans ce fichier :

```
# touch /opt/nfast/log/nfkm.log
# chmod 664 /opt/nfast/log/nfkm.log
```

Aucun retour n'est attendu sur ces deux commandes si elles ont réussies.

Néanmoins, ce fichier n'est pas forcément lu par tous les interpréteurs de commande (shells) il est donc recommandé de vérifier en se connectant avec l'utilisateur cible, puis d'exécuter la commande suivante :

```
# echo $NFKM_LOG
```

Résultat attendu :

```
/opt/nfast/log/nfkm.log
```

## 3 Paramétrage initial

### 3.1 Installation du service nfast

Toute communication avec le module netHSM se fait au travers d'un service TCP/IP. Il faut donc commencer par installer ce service (nommé nFast).

```
root@localhost bin]# /opt/nfast/sbin/install
Stopping any old nCipher server process.
I need to create the nfast user, in group nfast, with home directory /opt/nfast.
I can either:
1)Try to do it by editing /etc/passwd and /etc/group myself;
2)Try to use `adduser nfast' (this may sort of work on some systems);
3)Try to use `adduser --group --system nfast' a la Debian 2.2 and later;
4)Try to use `useradd -r nfast' a la at least Red Hat 5.0 and later;
5)Let you do it;
```

Dans le cas d'une RedHat, choisir l'option 4.  
Pour une Debian, préférée l'option 3.

```
Please type a number from 1 to 5: 4
Cleaning up /dev directory.
making privconn setuid and root
Setting up directories
Making default config file
Checking for SCSI hardware.
No SCSI devices found.
Checking for PCI hardware
No PCI devices found.
Installing startup scripts.
Warning: Installed, but no directly attached hardware was found. If
you have an nCipher PCI card or SCSI device, re-run `install' script
with hardware attached, or check `/proc/scsi/scsi' or `/proc/pci', or
consult nCipher support.
Starting nCipher server.
waiting for nCipher server to become operational ...
nCipher server now running
Installed.
```

L'installation ne doit pas poser de problème spécifique. Vérifiez néanmoins par la commande suivante que le service est effectivement bien activé. **Attention, sous Solaris, seule la ligne en caractères gras est visible.**

```
# ps -ef | grep nfast
root      31061      1  0 10:52 pts/2      00:00:00 su nfast -c ??set -e??echo $$
>hardserver.pid??date >&2??echo "Starting hardserver pid $$" >&2??exec
../sbin/hardserver -Llogfile?
nfast    31064 31061  0 10:52 pts/2      00:00:00 ../sbin/hardserver -Llogfile
root      31082     5144  0 10:54 pts/2      00:00:00 grep nfast
```

## 3.2 Récupération du ESN (Electronic Serial Number) et du Keyhash

Commande :

```
% /opt/nfast/bin/anonkneti <ADRESSE-IP-DU-NETHSM>
```

Retour attendu : <ESN> <KEYHASH>

Exemple de retour :

```
4213-33FF-AF1B d682e3d4257cb59d93f6f5ce7ccdb42c5ef16a4
```

**Attention** : cette commande doit être utilisée uniquement dans un réseau (IP) de confiance. Dans le cas contraire, ces informations peuvent être directement récupérées sur le module.

Si vous obtenez le message suivant, cela signifie que l'installation du service a échoué :

```
NFastApp_Connect failed: ServerNotRunning
```

## 3.3 Paramétrage du RFS (Remote File System)

Chaque boîtier nethSM doit être relié à un serveur – appelé RFS – pour y stocker les globs (fichiers chiffrés) des clés qui sont générés par le module. Si votre équipement HSM est déjà configuré pour une autre utilisation, vous ne devez pas recréer un autre serveur RFS.

```
% /opt/nfast/bin/rfs-setup <ADRESSE-IP-DU-NETHSM> <ESN> <KEYHASH>
```

Cette commande permet d'initialiser un système de fichier local.

Il faut à présent définir le serveur RFS sur le boîtier HSM, via le menu suivant :

- System ;
- Remote file system.

**Attention** que le pare-feu de RedHat ne bloque pas les ports entre le boîtier HSM et le serveur Linux

## 3.4 Définition du royaume de sécurité : création des cartes administrateur

Il s'agit maintenant de créer un nouveau royaume de sécurité. Pour cela, un accès physique au module nethSM est nécessaire.

### 3.4.1 Utilisation du boîtier

Accéder au menu suivant :

- Menu Security World Mgmt (3) ;
  - Module Initialization (3.2) ;
    - New Security World (3.2.1).

Deux nombres sont demandés : le premier correspond au nombre de cartes administrateur requis pour une opération ; le second correspond au nombre total de cartes administrateur générées.

Utiliser la touche tabulation pour passer d'un champ à l'autre.

À la question « *Specify all quorums?* », si vous répondez oui, il vous sera demandé le nombre de cartes administrateurs nécessaire pour chaque opération listée ci dessous. Si vous répondez non, le nombre de cartes administrateurs nécessaires sera le même pour toutes les opérations.

Un minimum de deux cartes est fortement recommandé.

Listes des opérations :

- Module reprogramming ;
- Key Recovery ;
- PIN Recovery ;
- NVRAM Access ;
- RTC access ;
- See debugging ;
- FTO (Foreign Token Open).

À la question « *Select security world module key type?* », sélectionner « **AES** ».

« *Do you want to make module 1 a valid target for remote share ?* », sélectionner « **YES** ».

Il faut alors introduire le nombre de cartes correspondant au second champ. Chaque carte peut être protégée par une *passphrase* optionnelle.

« *Give card a p'phrase ?* » Si vous souhaitez protéger la carte par une *passphrase*, répondre oui en cliquant sur B, sinon répondre en cliquant sur A.

Après l'insertion de la dernière carte, vous devriez obtenir le message suivant :

« *New security world successfully created* »

### 3.5 Création des cartes opérateurs

Pour créer les cartes opérateur, il faut un accès physique à l'équipement (néanmoins, un outil en ligne est disponible, mais l'opération de changement de carte étant toujours nécessaire, il est donc recommandé de se trouver près du module).

- Security World Management (3) :
  - CardSet Operations (3.5) :
    - Create OCS (3.5.1) (Operator Card Set) ;
  - « *Name for new card set:* », nommer le jeu de cartes (e.g. « **LINAGORA** ») ;
  - « *Specify OCS Quorum* », entrer le quorum (nombre de carte nécessaire pour effectuer une opération / nombre de cartes totales à créer) ;
  - « *Name individual cards ?* », si vous répondez « **yes** » à cette question, il vous sera demandé de nommer individuellement chaque carte insérée ;

- vous pouvez maintenant introduire les différentes cartes du jeu opérateur ; à chaque insertion, il vous sera demandé si vous souhaitez protéger la carte par une *passphrase*.

### 3.5.1 Utilisation de l'outil en ligne de commande

Il est possible d'utiliser les outils CLI fournis par nCipher pour créer le jeu de cartes opérateur :

```
% /opt/nfast/bin/createocs -m 1 -Q 1/3 -N LINAGORA
```

## 3.6 Configuration d'un client

La configuration d'un nouveau client (serveur autorisé à utiliser le netHSM) nécessite un accès physique à la machine. Sur le module, choisir le menu :

- System (1) ;
  - System Configuration (1.1) ;
    - Client Configuration (1.1.4) ;
      - New Client ;
      - et finalement fournir l'adresse IP du client.

Une fois cette opération effectuée, il faut exécuter la commande suivante depuis le client :

```
% /opt/nfast/bin/nethsmenroll <ADRESSE-IP-DU-MODULE> <ESN> <KEYHASH>
```

Retour attendu : **OK configuring hardserver's nethsm imports**

Puis, la commande :

```
% /opt/nfast/bin/config-serveratstartup
```

Retour attendu : *aucun message en cas de succès.*

## 3.7 Vérification du bon fonctionnement

Le bon fonctionnement de la communication entre le client et le module peut être vérifié par la commande suivante :

```
% /opt/nfast/bin/enquiry
[...]
Module #1:
[...]
mode                operational
[...]
```

Si vous obtenez bien ce message, votre module netHSM est prêt à fonctionner.

### 3.7.1 Création d'une clé de test

Il est également possible d'utiliser l'outil **generatekey** pour générer une clé pour vérifier le bon fonctionnement du module ainsi que pour valider la politique des cartes opérateur.

```
% /opt/nfast/bin/generatekey simple
```

```

protect: Protected by? (token, softcard, module) [token] >
recovery: Key recovery? (yes/no) [yes] >
type: Key type? (DES2, DES3, DH, DSA, HMACRIPEMD160, HMACSHA1, HMACSHA256,
      HMACSHA384, HMACSHA512, HMACTiger, RSA) [RSA] >
size: Key size? (bits, minimum 1024) [1024] >
OPTIONAL: pubexp: Public exponent for RSA key (in hex)? []
>
ident: Key identifier? [] > TEST3
plainname: Key name? [] > TEST3
nvrnm: Store blob in NVRAM (will require administrator cardset)? (yes/no) [no]
>
key generation parameters:
  operation      Operation to perform                generate
  application    Application                                simple
  protect        Protected by                                  token
  slot           Slot to read cards from                       0
  recovery       Key recovery                                  yes
  verify         Verify security of key                       yes
  type           Key type                                       RSA
  size           Key size                                       1024
  pubexp         Public exponent for RSA key (in hex)
  ident          Key identifier                                TEST3
  plainname      Key name                                       TEST3
  nvrnm          Store blob in NVRAM (will require administrator cardset) no

Loading `LINAGORA':
  Module 1: 0 cards of 1 read
  Module 1 slot 0: empty
Insert/change card(s) (or change module mode).

```

Comme vous pouvez le constater, le module demande l'insertion d'une carte du jeu Linagora.

**Note :** la *passphrase* doit être fourni sur l'ordinateur.

## 4 Redémarrage des serveurs

### 4.1 Serveur RFS

Si votre système utilise un système de fichier `/dev` dynamique (e.g. c'est le cas de RedHat Enterprise 4), il est nécessaire de relancer le script `« /opt/nfast/sbin/install »` après chaque redémarrage (`reboot`). En effet, les fichiers périphériques (`/dev/nfast`) étant statiques, ils ne sont pas recréés au démarrage.

Aucune manipulation n'est nécessaire si le serveur RFS est installé sur un serveur utilisant le système d'exploitation Solaris.

### 4.2 Périphérique netHSM

Le redémarrage du périphérique netHSM nécessite la réactivation du royaume de sécurité – à l'aide la commande `preload`. En effet, l'exécutable `preload` refusera de démarrer l'application si les pilotes de périphériques n'arrivent pas à joindre le module HSM. Bien entendu, un accès physique au module HSM est nécessaire pour y introduire le nombre de cartes nécessaire du jeu de carte opérateurs (déterminé à sa création).

Cette réactivation doit être effectuée via la commande suivante :

```
% /opt/nfast/bin/preload -c <NOM-DU-JEU-DE-CARTES-OPERATEURS> pause
```

Retour attendu :

```
Loading '<nom du jeu de carte opérateur>'
[....]
Card reading complete.
```

Exemple de retour :

```
Loading `LINAGORA':
Module 1 slot 0: empty
Module 1 slot 0: `LINAGORA' #2
Module 1 slot 0:- passphrase supplied - reading card
Module 1 slot 0: `LINAGORA' #2: already read
Module 1 slot 0: empty
Module 1 slot 0: `LINAGORA' #1
Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.
```

Une fois ce message obtenu, il faut maintenant procéder à la réactivation des autorités de certification dans EJBCA, cette procédure est décrite dans le chapitre suivant.

## 4.3 Redémarrage du serveur applicatif

### 4.3.1 Vérification de la communication entre les pilotes et le module HSM

Si vous souhaitez redémarrer le serveur applicatif (par exemple, JBoss), aucune manipulation n'est nécessaire si le module est opérationnel. Pour vérifier si celui-ci est effectivement bien activé, on peut utiliser la commande `preload` de la manière suivante :

```
-bash-3.00$ /opt/nfast/bin/preload echo "ok"
```

Résultat attendu :

```
Executing echo ok  
ok
```

Si la commande renvoie le message suivant :

```
10:05:39 WARNING: Module #2: Module has failed  
No usable modules
```

Il est nécessaire d'attendre que le périphérique HSM soit opérationnel (fin de la phase de démarrage).

### 4.3.2 Activation des AC

Chaque autorité de confiance dont la clé est gérée par le module HSM doit être réactivée via l'interface d'administration d'EJBCA. Pour activer une autorité de confiance, procéder de la manière suivante :

- se connecter sur l'interface d'administration d'EJBCA ;
- cliquez sur le menu « Fonctions de base » ;
- pour chaque autorité de confiance gérée par le HSM, cliquez sur le lien « Information sur l'AC » correspondant ;
- fournir la *passphrase* de la carte présente dans le lecteur de l'équipe HSM dans la case « Code d'authentification », puis cliquez sur le bouton « Activer ».

## 5 Utilisation du netHSM pour EJBCA

### 5.1 Activation du service netHSM sur le serveur RFS

Éditer le fichier « `/opt/nfast/kmdatat/config/config` » pour ajouter les lignes suivantes dans la section « `[server_startup]` ».

```
nonpriv_port=9000  
priv_port=9001
```

### 5.2 Compilation d'EJBCA

Cette étape nécessite de configurer et d'installer EJBCA. Pour ce faire, ce reporter au document d'installation d'EJBCA en mode pré-production. Une fois la fin de la configuration et de l'installation reporter de nouveau à ce document pour continuer la cérémonie de clés.

## 6 Création d'une clé pour génération d'un certificat racine

Pour générer une autorité de certification (AC) dans EJBCA en utilisant l'équipement netHSM, il faut d'abord générer une clé en utilisant les bibliothèques fournies avec les pilotes netHSM. Le script suivant permet une utilisation similaire à la commande « `keytool` ».

### 6.1 Création de la clé racine

#### 6.1.1 Présentation de l'utilitaire de génération de clés

**Attention :** ce script est prévu pour être utilisé avec un JRE en version 1.5. Si vous voulez l'utiliser avec un JRE en version 1.4, il faut renommer le fichier « `bcprov-jdk15.jar` » en « `bcprov-jdk14.jar` ».

Le script « `keytoolncipher.sh` » :

```
#!/bin/bash

if [ -z $EJBCA_HOME ]; then
    echo "Fatal error: EJBCA_HOME is not set"
    exit 1
fi

if [ -z $JAVA_HOME ]; then
    echo "Fatal error: JAVA_HOME is not set"
fi

if [ -z $NFAST_HOME ]; then
    echo "Warning: NFAST_HOME not set, using default to /opt/nfast"
    NFAST_HOME=/opt/nfast
fi

NFAST_JARS=$NFAST_HOME/java/classes

CLASSES=$EJBCA_HOME/lib/bcprov-jdk15.jar
CLASSES=$CLASSES:$EJBCA_HOME/tmp/bin/classes
# use this instead if you want build from eclipse
#CLASSES=$CLASSES:$EJBCA_HOME/out/classes

# Add nfast's JARs to classpath
for jar in rsaprivenc.jar nfjava.jar kmjava.jar kmcsp.jar jutils.jar
do
    CLASSES="$CLASSES:$NFAST_JARS/$jar"
done

# Prepare arguments
args="$0 $1"
shift
args="$args com.ncipher.provider.km.nCipherKM nCipher.sworld $@"

# Finally run java
$JAVA_HOME/bin/java -cp $CLASSES org.ejbca.ui.cli.HSMKeyTool $args
```

## 6.1.2 Utilisation du script « `keytoolncipher.sh` » pour créer la clé

Commande :

```
% /opt/nfast/bin/preload -c <nom du jeu de carte opérateur> pause
[...]
Loading `LINAGORA':
Module 1 slot 0: empty
Module 1 slot 0: `LINAGORA' #2
Module 1 slot 0:- passphrase supplied - reading card
Module 1 slot 0: `LINAGORA' #2: already read
Module 1 slot 0: empty
Module 1 slot 0: `LINAGORA' #1
Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.

Loading complete; now pausing
```

Une fois la ligne précédente obtenue, ouvrir un nouveau terminal et exécuter les commandes suivantes :

```
% export EJBCA_HOME=/opt/ejbca
% cd $EJBCA_HOME/
% /opt/nfast/bin/preload $EJBCA_HOME/bin/nCipherHSM.sh generate 4096 defaultRoot
```

Le paramètre « `defaultRoot` » correspond au nom de la clé ; sa valeur sera utilisée pour la création du certificat depuis EJBCA.

Retour attendu : empreinte numérique (hash) de la clé générée

Exemple de retour :

```
[...]
Creating certificate with entry defaultRoot in KeyStore of type nCipher.sworld with
provider nCipherKM.
Next line will contain the identity identifying the keystore:
58bc95f359f8dbe31282e06504e8970ac2d6b481
```

Si vous obtenez le message suivant :

```
com.ncipher.provider.nCRuntimeException:
com.ncipher.km.nfkm.nfkmCommunicationException nfkmcmdadp: NFKM_LOG environment
variable, if set, must point to a file
```

... il faut créer un fichier de journal (*log*) et définir la variable `NFKM_LOG`, en fonction du système d'exploitation cible. Exemple de création du fichier de journal :

```
# touch /opt/nfast/log/nfkm.log
# chown nfast:nfast /opt/nfast/log/nfkm.log
# chmod 664 /opt/nfast/log/nfkm.log
# export NFKM_LOG=/opt/nfast/log/nfkm.log
```

## 6.2 Création du certificat dans EJBCA

Pour utiliser un quorum de cartes opérateurs supérieur à 1, vous devez utiliser l'outil `preload` fourni dans les pilotes netHSM pour démarrer JBoss. En effet, cet outil permet via la ligne de commande, de procéder au chargement du nombre nécessaire de cartes.

### 6.2.1 Modification du script de démarrage de RedHat

Éditer le fichier « `/etc/init.d/jboss` » de façon à obtenir la ligne suivante :

```
JBOSSSH=${JBOSSSH:-"/opt/nfast/bin/preload $JBOSS_HOME/bin/run.sh -c $JBOSS_CONF -b $JBOSS_HOST"}
```

### 6.2.2 Création du certificat

Si la création de l'autorité de certification (AC) ne fonctionne pas, **vérifier que l'utilisateur qui démarre le service JBoss appartient au groupe `nfast`**. Il peut être nécessaire de modifier les droits sur les fichiers suivants :

```
# mkdir /opt/nfast/log
# chmod 664 /opt/nfast/log/cmdadp-debug.log
# chmod 664 /opt/nfast/log/cmdadp.log
```

Pour créer une nouvelle AC dans EJBCA, vous devez disposer des éléments suivants :

- l'empreinte numérique (hash) de la clé ;
- le nom de la clé ;
- le mot de passe de la carte opérateur présente dans le lecteur.

Une fois les pré-requis remplis, procéder aux manipulations suivantes :

1. Se connecter à l'interface d'administration d'EJBCA ;
2. Cliquer sur « Éditer/créer AC » ;
3. Donner le nom de l'AC à créer ;
4. Cliquer sur l'AC puis sur « Éditer » ;
5. Choisir « NFastCAToken » comme support du certificat de l'AC ;
6. Dans le champ « propriété », saisir (sur deux lignes distinctes) les lignes suivantes :
  - « `keyStore <NUMÉRO-HEXADÉCIMAL-DU-KEYSTORE>` »,
  - « `defaultKey <NOM-DONNÉ-LORS-DE-LA-GÉNÉRATION-DE-LA-CLÉ>` » ;
7. Spécifier le code PIN de la carte présente dans le netHSM pour le code d'authentification.

Type of CA	X509
CA Token Type	NFastCAToken
Hard CA Token Properties	keyStore 08b5549a1412a65ad11e948a9c8c5e10dc4e2c74 defaultKey defaultRoot
Authentication Code	*****
Signing Algorithm	SHA1WithRSA
Subject DN	cn=OJBCA Root Authority, C=FR
Signed By	Self Signed
Certificate Profile	ROOTCA
Validity (Days)	1095
Description	

## 7 Suppression d'un royaume de sécurité

**Attention :** les cartes opérateurs ne sont pas ré-inscriptibles. Si vous souhaitez réinstaller votre nethSM ou supprimer le royaume de sécurité, **vous devez impérativement effacer les cartes opérateurs avant de supprimer le royaume de sécurité.** Dans le cas contraire, vous ne pourrez plus utiliser les cartes opérateurs.

Pour plus d'information, reportez vous à la documentation de nCipher :  
« *nethSM Operator Guide* », chapitre 4, section « *Erasing operator cards and softcards* ».

## 8 Références documentaires

### Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE
EJBCA : INSTALL	1.2	9999-02	EJBCA – Guide d'installation

### Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB