

Guide d'installation d'un HSM TrustWay

EJBCA

EJBCA, Bull TrustWay

Version 1.0

Le 23/10/2009

Identifiant : -

Fichier original : 9999-02_DOC_EJBCA_Guide-Installation-TrustWay_1.0.odt

Historique des évolutions et visas

Visas

	RÉDACTION	APPROBATION	VALIDATION
NOM	André PELLÉ	David CARELLA	
FONCTION	Administrateur système	Expert PKI	
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	23/10/2009	David CARELLA	Création basée sur un document existant rédigé par André PELLÉ.
0.2	23/10/2009	David CARELLA	Relecture et corrections
1.0	23/10/2009	David CARELLA	Finalisation

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 : Publicque

NOM	ORGANISME	POUR	MÉDIA

Liste des contributeurs

André PELLÉ, David CARELLA.

Table des matières

1	Introduction.....	6
2	Installation du driver.....	7
2.1	Installation du driver « CC2000 ».....	7
2.2	Adaptation du système.....	7
3	Installation de la carte HSM TrustWay.....	9
3.1	Initialisation de la carte TrustWay.....	9
3.2	Configuration pour utiliser la carte TrustWay avec EJBCA.....	9
3.3	Utilisation de la carte TrustWay avec EJBCA.....	9
4	Sigles et acronymes.....	11
5	Références.....	12

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 ...

1 Introduction

L'objet du présent document est la description de l'installation de la carte HSM (*Hardware Security Module*) BULL cc2000 TrustWay ainsi que de son utilisation avec l'application de PKI EJBCA dans un environnement DEBIAN Etch.

En pré-requis de cette installation, il faut avoir à disposition une machine et un environnement DEBIAN Etch ainsi qu'EJBCA, par exemple en ayant respecté le document *Guide d'installation EJBCA sous DEBIAN*.

2 Installation du *driver*

2.1 Installation du *driver* « CC2000 »

L'installation du pilote (*driver*) s'effectue de la manière suivante.

Introduire le CD-ROM BULL TrustWay CC2000 et copier le fichier « `linux` » dans le répertoire « `/home/linagora` » par exemple :

```
# mkdir /home/linagora
# mount /media/cdrom
# cp -r /media/cdrom/linux /home/linagora
```

Éditer le fichier « `JRE.txt` » :

```
# cd /home/linagora/linux
# touch JRE.txt
# echo '/opt/java' >> JRE.txt
```

Exécuter la ligne suivante pour lancer l'installation du pilote :

```
# /home/linagora/linux/install
On which directory do we put cc2000 DRIVER sources and PKCS11 includes (full pathname)
[default pathname is /usr/local/cc2000] ?
/home/linagora/cc2000
Enter the full pathname of Administraton Application installation [default pathname is
/usr/local/TrustWay] :
/home/test/TrustWay
```

Il faut veiller à spécifier le répertoire d'installation du pilote. Dans notre exemple, nous désignons les répertoires « `/home/linagora/cc2000` » et « `/home/linagora/TrustWay` ».

À la question concernant la présence de Java sur la machine, il faut répondre oui. Il faut également veiller à spécifier le répertoire contenant Java :

```
Is Java Runtime Environment (JRE) installed on your machine ? [y/n]
Y
Enter the full pathname of the JRE (or control-c to abort):
/opt/java
```

2.2 Adaptation du système

Le pilote (*driver*) de la carte TrustWay entre en conflit avec le module `i2o_core` chargé au démarrage de la DEBIAN Etch. Il faut tout d'abord procéder à la désactivation de ce module avant de pouvoir utiliser la carte.

Tout d'abord, il faut veiller à inhiber les modules `i2o_core` et `cc2000` à l'aide de la commande suivante :

```
# modprobe -r i2o_core
# modprobe -r cc2000
```

Puis, lancer la commande suivante :

```
# dpkg-reconfigure linux-image-<VERSION>
```

Où <VERSION> représente la version du noyau Linux utilisé. La commande suivante permet de récupérer la version du noyau Linux utilisé :

```
# uname -r
```

À l'issue de cette étape, une nouvelle image de `initrd.img` a été créée dans le répertoire « `/boot` ».

Pour finir l'installation du pilote, il faut éditer le fichier `rc.local` situé dans le dossier `/etc` à l'aide de la commande suivante :

```
# vi /etc/rc.local
```

Ajouter les deux lignes suivantes avant l'occurrence « `exit 0` » comme suit :

```
[ -c /dev/cc2000 ] || mknod -m 666 /dev/cc2000 c 200 0  
modprobe --force cc2000
```

Cette opération permet le chargement automatique au démarrage du module du pilote de la carte TrustWay.

Le pilote est maintenant installé.

3 Installation de la carte HSM TrustWay

3.1 Initialisation de la carte TrustWay

Cette section est décrite dans la documentation livrée avec la carte TrustWay sur le CD-ROM d'installation. Le document est intitulé « `Manuel_Installation_Carte_TrustWay_PCI.pdf` » et se trouve dans le répertoire « `Documentation/French/` » du CD-ROM d'installation.

3.2 Configuration pour utiliser la carte TrustWay avec EJBCA

Cette section décrit les opérations à effectuer afin que l'application EJBCA puisse utiliser la carte TrustWay.

Créer le fichier « `trustWay.cfg` » dans le dossier « `/opt/ejbca/bin` » :

```
# touch trustWay.cfg
```

Éditer le fichier « `/opt/ejbca/bin/trustWay.cfg` » et ajouter les lignes suivantes :

```
# vi /opt/ejbca/bin/trustWay.cfg
```

Le fichier « `trustWay.cfg` » doit contenir les lignes suivantes :

```
name=TrustWay
library=/usr/lib/libgpkcs11cc2000.so
slotListIndex=0
attributes(generate,CKO_PRIVATE_KEY,*) = {
    CKA_TOKEN = true
}
```

Une fois le fichier « `trustWay.cfg` » sauvegardé, il faut générer une clé privée pour l'AC. Pour réaliser cette opération, il faut exécuter la commande suivante :

```
# LD_LIBRARY_PATH=/usr/lib ./pkcs11HSM.sh generate ./trustWay.cfg 2048 testkey
```

L'alias « `testkey` » représente le nom donné à la clé privée. Vous pouvez utiliser le nom d'alias que vous souhaitez pour faire référence à la clé privée de votre AC.

3.3 Utilisation de la carte TrustWay avec EJBCA

Cette section décrit la façon d'utiliser la carte TrustWay avec EJBCA.

Il faut, dans un premier temps, se connecter à l'interface d'administration de la PKI (opération décrite dans le document *Guide d'installation EJBCA sous DEBIAN*).

Aller dans la section « Éditer/créer une autorité de certification ».

Compléter le champ « Ajouter » avec le nom de la future AC. Dans notre exemple « `ACtest` ». Puis cliquer sur le bouton « Créer ».

Au niveau du champ « Type de token d'AC » sélectionner « `PKCS #11` ».

Compléter le champ « Propriété du Token HSM » comme suit :

```
defaultKey testkey
certSignKey testkey
crlSignKey testkey
sharedLibrary /usr/lib/libgpkcs11cc2000.so
slotListIndex 0
pin
```

Compléter le champ « Durée de validité (jours) » avec le nombre de jours de validité de l'AC ainsi que le champ « DN du sujet ».

Format de l'AC	X509
Token du certificat de l'AC	PKCS#11
Propriétés du token matériel de l'AC	<pre>defaultKey mytestkey certSignKey mytestkey crlSignKey mytestkey sharedLibrary /usr/lib/libgpkcs11cc2000.so slotListIndex 0 pin</pre>
Code d'authentification	
Algorithme de signature	SHA1WithRSA
DN du sujet	CN=ACtest,O=EJBCA,C=FR
Signé par	Auto-signé
Profil de certificats	ROOTCA
Durée de validité (jours)	720

Cliquer le bouton « Créer » en bas de la page pour effectuer l'opération de génération du certificat de l'autorité de certification.

4 Sigles et acronymes

Sigle	Désignation
AC	Autorité de certification
EJBCA	Enterprise Java Beans Certificate Authority
HSM	Hardware Security Module
PKI	Public Key Infrastructure

5 Références

Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE OU IDENTIFIANT

Références externes

RÉFÉRENCE	VER.	ÉDITEUR	TITRE OU IDENTIFIANT

Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB