

Paramétrage d'EJBCA

PKI crypto

EJBCA 3.8.0 [fr]

Version 1.0

Le 03/11/2008

Identifiant : DOC_PKI-crypto_Parametrage-EJBCA_1.0

Fichier original : 3058-01_DOC_PKI-crypto_Parametrage-EJBCA_1.0.odt

Historique des évolutions et visas

Visas

	RÉDACTION	APPROBATION	VALIDATION
NOM	André PELLÉ	David CARELLA	Yannick QUENEC'H DU
FONCTION	Administrateur Système & Réseau	Expert PKI	Responsable du Pôle Sécurité
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	29/08/2008	André PELLÉ	Création
0.2	29/08/2008	André PELLÉ	Rédaction
0.3	10/09/2008	David CARELLA	Relecture et corrections
1.0	03/11/2008	David CARELLA	Approbation et 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 : **Client du projet**

NOM	ORGANISME	POUR	MÉDIA
Tous les collaborateurs	Groupe Linagora	Information	GED
Collaborateurs du projet		Action	Courriel

Liste des contributeurs

André PELLÉ, David CARELLA.

Informations générales

Ordre de lecture (ce document apparaît sur fond rouge) :

ORDRE	VER.	PROJET	TITRE
01	1.0	3058-01	Installation EJBCA
02	1.0	3058-01	Installation EJBCA haute disponibilité
03	1.0	3058-01	Configuration EJBCA avec appliance LunaSA SafeNet
04	1.0	3058-01	Paramétrage EJBCA

Table des matières

1	Introduction.....	7
2	Paramétrage système.....	8
2.1	Recouvrement de clés.....	8
2.2	Production de tokens matériels.....	8
3	Définition des profils de certificats.....	9
3.1	Profil du certificat d'une AC racine.....	9
3.2	Profil de certificats finaux.....	11
4	Définition du profil d'entités.....	14
5	Sigles et acronymes.....	16
6	Références.....	17

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 ...

1 Introduction

Ce document présente un paramétrage typique d'EJBCA pour des profils de certificats et d'entités, qui serviront à créer des certificats finaux de chiffrement.

2 Paramétrage système

2.1 Recouvrement de clés

Il faut se rendre dans l'interface d'administration d'EJBCA et cliquer sur le lien « Configuration du système » du menu « Fonctions système ». Dans ce menu, il faut sélectionner l'option « Activer le recouvrement de clés », puis enregistrer.

2.2 Production de tokens matériels

Il faut se rendre dans l'interface d'administration d'EJBCA et cliquer sur le lien « Configuration du système » du menu « Fonctions système ». Dans ce menu, il faut sélectionner l'option « Production de tokens matériels », puis enregistrer.

3 Définition des profils de certificats

3.1 Profil du certificat d'une AC racine

Le tableau ci-après contient la description du profil de certificats pour un certificat d'autorité de certification (AC) racine.

Ce profil de certificats (*Certificate Profile*) est nommé : **CP_ROOTCA**.

Champ	Description
Durée de validité (jours)	11688 (32 ans)
Autoriser la surcharge de la validité (requête CMP)	non (non coché)
Autoriser la surcharge d'extensions (requête CMP)	non (non coché)
Utiliser les contraintes de base (Basic Constraints)	oui (coché)
Contraintes de base (Basic Constraints) à critique	oui (coché)
Utiliser la contrainte de longueur de chemin de certification	non (non coché)
Utiliser les usages de clé (Key Usage)	oui (coché)
Usages de clé (Key Usage) à critique	oui (coché)
Utiliser l'identifiant de la clé publique du sujet (Subject Key Identifier)	oui (coché)
Utiliser l'identifiant de la clé publique de l'émetteur (Authority Key Identifier)	oui (coché)
Utiliser un nom alternatif du sujet (Subject Alternative Name)	non (non coché)
Nom alternatif du sujet (Subject Alternative Name) à critique	non (non coché)
Utiliser des attributs d'annuaire du sujet (Subject Directory Attributes)	non (non coché)
Utiliser les points de distribution de LCR (CRL Distribution Points)	non (non coché)
Points de distribution de LCR (CRL Distribution Points) à critique	non (non coché)
Utiliser un point de distribution de LCR déjà défini pour une AC	non (non coché)
URI d'un point de distribution de LCR	laisser vide
Nom distinctif de l'émetteur de la LCR (CRL Issuer)	laisser vide
Utiliser les points de distribution de delta LCR (Freshest CRL)	non (non coché)
Utiliser l'extension Freshest CRL définie pour l'AC	non (non coché)
URI d'un point de distribution de delta LCR (Freshest CRL)	laisser vide

Champ	Description
Utiliser OCSP sans vérification (de signature)	non (non coché)
Utiliser les accès aux informations de l'émetteur (Authority Information Access)	non (non coché)
Utiliser un serveur OCSP défini pour une AC	non (non coché)
URL du service OCSP	non (non coché)
Utiliser les politiques de certification	oui (coché)
Politiques de certification à critique	non (non coché)
Identifiant (OID) de la politique de certification	1.2.250.1.124.3.1.1.1
Notification utilisateur	laisser vide
URI de la politique de certification	laisser vide
Utiliser les certificats qualifiés	non (non coché)
Utiliser les déclarations de certificats qualifiés (QC Statements)	non (non coché)
Déclarations de certificats qualifiés (QC Statements) à critique	non (non coché)
Utiliser la déclaration PKIX QCSyntax-v2 (profils de certificats qualifiés v2)	non (non coché)
Identifiant de sémantique (Semantics Identifier) (OID)	laisser vide
Nom de l'AE	laisser vide
Utiliser la conformité ETSI CQ	non (non coché)
Utiliser le dispositif de création de signature sécurisé ETSI	non (non coché)
Utiliser la limite de valeur de transaction ETSI	non (non coché)
Devise de la Limite de valeur	laisser vide
Quantité de la Limite de valeur	laisser vide
Exposant de la Limite de valeur	laisser vide
Utiliser une chaîne QC-statement personnalisée	non (non coché)
OID QC-statement personnalisé	laisser vide
Texte QC-statement personnalisé	laisser vide
Usages de clé (Key Usage)	Type d'utilisation de clé : Signature de certificats (keyCertSign) Signature de LCR (cRLSign)
Autoriser la surcharge des usages de clé (Key Usage)	non (non coché)
Utiliser les usages de clé étendus (Extended Key Usage)	non (non coché)
Usages de clé étendus (Extended Key Usage) à critique	non (non coché)
Usages de clé étendus (Extended Key Usage)	laisser vide
Droits d'accès CVC	ne rien modifier
Utiliser un gabarit (template) MS	non (non coché)

Champ	Description
Valeur du gabarit (template) Microsoft	non
Utiliser le suffixe de CN	non (non coché)
Suffixe de CN Texte apposé à la fin du premier attribut CN	laisser vide
Utiliser les sous-éléments du DN du sujet	non (non coché)
Sous-éléments du DN du sujet	non
Utiliser les sous-éléments du nom alternatif	non (non coché)
Sous-éléments du nom alternatif du sujet	non (non coché)
Tailles de clé disponibles	4096 bits
AC disponibles	aucune
Services de publication	aucun
Type	AC racine

Remarque : selon la DCSSI : « Pour une utilisation au-delà de [l'année] 2020, la taille minimale du module est de 4096 bits. ».

3.2 Profil de certificats finaux

Le tableau ci-après contient la description du profil de certificats pour les certificats finaux.

Ce profil de certificats (*Certificate Profile*) est nommé : **CP_ENDUSER_CRYPTO**.

Champ	Description
Durée de validité (jours)	1461 (4 ans)
Autoriser la surcharge de la validité (requête CMP)	oui (coché)
Autoriser la surcharge d'extensions (requête CMP)	non (non coché)
Utiliser les contraintes de base (Basic Constraints)	oui (coché)
Contraintes de base (Basic Constraints) à critique	oui (coché)
Utiliser la contrainte de longueur de chemin de certification	non (non coché)
Utiliser les usages de clé (Key Usage)	oui (coché)
Usages de clé (Key Usage) à critique	oui (coché)
Utiliser l'identifiant de la clé publique du sujet (Subject Key Identifier)	oui (coché)
Utiliser l'identifiant de la clé publique de l'émetteur (Authority Key Identifier)	oui (coché)
Utiliser un nom alternatif du sujet (Subject Alternative Name)	non (non coché)
Nom alternatif du sujet (Subject Alternative Name) à critique	non (non coché)
Utiliser des attributs d'annuaire du sujet (Subject Directory Attributes)	non (non coché)

Champ	Description
Utiliser les points de distribution de LCR (CRL Distribution Points)	oui (coché)
Points de distribution de LCR (CRL Distribution Points) à critique	non (non coché)
Utiliser un point de distribution de LCR déjà défini pour une AC	non (non coché)
URI d'un point de distribution de LCR	<code>ldap://ldap.sogepass.socgen/CN=crypto,OU=SoGePass,O=SG?certificateRevocationList;http://crl.sogepass.socgen/?crlname=crypto;http://crl.sogepass.net/crl/crypto.crl</code>
Nom distinctif de l'émetteur de la LCR (CRL Issuer)	laisser vide
Utiliser les points de distribution de delta LCR (Freshest CRL)	oui (coché)
Utiliser l'extension Freshest CRL définie pour l'AC	non (non coché)
URI d'un point de distribution de delta LCR (Freshest CRL)	<code>ldap://ldap.sogepass.socgen/CN=delta-crypto,OU=SoGePass,O=SG?certificateRevocationList;http://crl.sogepass.socgen/?crlname=delta-crypto;http://crl.sogepass.net/crl/delta-crypto.crl</code>
Utiliser OCSP sans vérification (de signature)	non (non coché)
Utiliser les accès aux informations de l'émetteur (Authority Information Access)	oui (coché)
Utiliser un serveur OCSP défini pour une AC	oui (coché)
URL du service OCSP	laisser vide
URI de l'AC émettrice	laisser vide
Utiliser les politiques de certification	oui (coché)
Politiques de certification à critique	non (non coché)
Identifiant (OID) de la politique de certification	1.2.250.1.124.3.1.7.1
Notification utilisateur	laisser vide
URI de la politique de certification	laisser vide
Utiliser les certificats qualifiés	non (non coché)
Utiliser les déclarations de certificats qualifiés (QC Statements)	non (non coché)
Déclarations de certificats qualifiés (QC Statements) à critique	non (non coché)
Utiliser la déclaration PKIX QCSyntax-v2 (profils de certificats qualifiés v2)	non (non coché)
Identifiant de sémantique (Semantics Identifier) (OID)	laisser vide
Nom de l'AE	laisser vide
Utiliser la conformité ETSI CQ	non (non coché)
Utiliser le dispositif de création de signature sécurisé ETSI	non (non coché)
Utiliser la limite de valeur de transaction	non (non coché)

Champ	Description
ETSI	
Devise de la Limite de valeur	laisser vide
Quantité de la Limite de valeur	laisser vide
Exposant de la Limite de valeur	laisser vide
Utiliser une chaîne QC-statement personnalisée	non (non coché)
OID QC-statement personnalisé	laisser vide
Texte QC-statement personnalisé	laisser vide
Usages de clé (Key Usage)	Type d'utilisation de clé : Signature numérique (digitalSignature) Chiffrement de clés (keyEncipherment)
Autoriser la surcharge des usages de clé (Key Usage)	oui (coché)
Utiliser les usages de clé étendus (Extended Key Usage)	oui (coché)
Usages de clé étendus (Extended Key Usage) à critique	non (non coché)
Usages de clé étendus (Extended Key Usage)	Protection de courriel (emailProtection) MS Encrypted File System (système de fichiers chiffré)
Droits d'accès CVC	DG3 et DG4
Utiliser un gabarit (template) MS	non (non coché)
Valeur du gabarit (template) Microsoft	non
Utiliser le suffixe de CN	non (non coché)
Suffixe de CN	laisser vide
Utiliser les sous-éléments du DN du sujet	non (non coché)
Sous-éléments du DN du sujet	non
Utiliser les sous-éléments du nom alternatif	non (non coché)
Sous-éléments du nom alternatif du sujet	non (non coché)
Tailles de clé disponibles	1024 bits, 2048 bits (cf. remarque ci-après)
AC disponibles	Toutes les AC
Services de publication	aucun
Type	Entité : certificat final (client ou serveur).

Attention : les clés de 1024 bits ne sont plus considérées comme robustes selon l'état de l'art en cryptographie. Selon la DCSSI : « Il est recommandé d'employer des modules d'au moins 2048 bits, même pour une utilisation ne devant pas dépasser [l'année] 2010. ».

4 Définition du profil d'entités

Le tableau ci-après contient la description du profil d'entités, pour les entités de certificat final.

Ce profil d'entités (*Entity Profile*) est nommé : **EP_ENDUSER_CRYPTO**.

Champ	Description
Nom	Ce champ permet de spécifier un nom ou de laisser l'utilisateur le saisir lors de la demande : cocher « requis » et « modifiable ».
Mot de passe	Ce champ permet à l'utilisateur de saisir un mot de passe, utile pour les fichiers PKCS #12 : <ul style="list-style-type: none"> – l'IGC peut générer le mot de passe aléatoirement et l'envoyer par courrier électronique (dans ce cas, cocher la case « Auto-généré ») ; – il est également possible d'imprimer ce mot de passe ; – saisir « requis » si le champ est obligatoire lors de la saisie par l'utilisateur.
Génération par lot	cocher « Utiliser » uniquement
Champ DN du sujet	Liste des champs à ajouter au sujet du DN du certificat : <ul style="list-style-type: none"> – UID, Identifiant unique (requis, modifiable) – CN, Nom commun (requis, modifiable) – OU, Unité d'organisation (modifiable) – O, Organisation (raison sociale) (requis, non modifiable), O=GROUPE SOCIETE GENERALE – C, Pays (ISO 3166) (requis, non modifiable), C=FR
Champ pour le nom alternatif du certificat	Spécifier comme nom alternatif au certificat (en relation avec le profil de certificats) : <ul style="list-style-type: none"> – Nom RFC 822 (adresse de courriel) Cocher « Utiliser l'adresse de courriel de l'entité » uniquement.
Inverser DN du sujet et le Nom Alternatif du sujet	non coché
Domaine du courrier électronique	cocher « utiliser » et « modifiable » uniquement
Champs Attribut du sujet d'annuaire (Subject Directory Attribute)	laisser par défaut
Date de début de validité du certificat	Laisser vide
Date de fin de validité du certificat	Laisser vide
Profil de certificats par défaut	Sélectionner « CP_ENDUSER_CRYPTO »
Profils de certificats disponibles	Sélectionner « CP_ENDUSER_CRYPTO »
AC par défaut	Ce champ permet de définir l'AC qui sera utilisée par défaut par le profil d'entités.
AC disponibles	Ce champ permet de sélectionner les AC que l'on souhaite pouvoir utilisées avec ce profil d'entités.
Token par défaut	Sélectionner « Fichier P12 (PKCS #12) »
Tokens disponibles	Sélectionner « Fichier P12 (PKCS #12) »
Utiliser des émetteurs de tokens matériels	non (non coché)
Émetteur de token matériel par défaut	laisser vide
Émetteurs de token matériel	laisser vide

Champ	Description
disponibles	
Nombre de requêtes acceptées	laisser vide
Type :	
Clé recouvrable	cocher « requis », « défaut » et « utiliser »
Permettre la fusion des attributs du DN (WebService)	oui (coché)
Service : Envoyer la notification par courriel	
Envoyer la notification par courriel	ne rien cocher
Adresse de courriel de l'expéditeur	laisser vide
Adresse de courriel du destinataire	laisser vide
Événements déclencheurs de la notification	ne rien modifier
Sujet du courriel de notification	laisser vide
Message du courriel de notification	laisser vide
Service : Impression des données utilisateur	
Impression des données utilisateur	ne rien cocher
Nom de l'imprimante	ne rien faire
Nombre de copies	ne rien faire
Gabarit actif	champ d'information
Ajouter gabarit	ne rien faire

5 Sigles et acronymes

Sigle	Désignation
AC	Autorité de certification
AE	Autorité d'enregistrement
CA	Certificate Authority
CMP	Certificate Management Protocol
CN	Common Name
CP	Certificate Policy
CQ	Certificat qualifié
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVC	Card Verification Code
DC	Domain Component
DER	Distinguished Encoding Rules
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
EJB	Enterprise JavaBeans
EJBCA	EJB Certificate Authority
IGC	Infrastructure de gestion de clés [fr-FR]
JKS	Java Key Store
LCR	Liste des certificats révoqués
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
OID	Object Identifier
OU	Organizational Unit
PC	Politique de certification
PEM	Privacy Enhancement for Internet Electronic Mail
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure [en-US], [en]
QC	Qualified Certificate
RA	Registration Authority
RSA	Rivest, Shamir, Adleman (algorithme asymétrique)
SHA-1	Secure Hash Algorithm One
SHA-256	Secure Hash Algorithm 256
SP	Service de publication
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

6 Références

Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE
EJBCA : INSTALL	1.0	3058-01	Assistance EJBCA – Guide d'installation

Références externes

RÉFÉRENCE	VER.	ÉDITEUR	TITRE

Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB