



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information

## **Rapport de certification ANSSI-CC-2012/47**

### **EJBCA, version 5.0.4**

*Paris, 4 octobre 2012*

*Le directeur général de l'agence nationale  
de la sécurité des systèmes d'information*

Patrick Pailloux  
[ORIGINAL SIGNE]



## Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information  
Centre de certification  
51, boulevard de la Tour Maubourg  
75700 Paris cedex 07 SP

[certification.anssi@ssi.gouv.fr](mailto:certification.anssi@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	<b>ANSSI-CC-2012/47</b>
Nom du produit	<b>EJBCA, version 5.0.4</b>
Conformité à un profil de protection	<b>[PP-CIMC] : Certificate Issuing and Management Components Family of Protection Profiles, Security Level 3 Version 1.0</b>
Critères d'évaluation et version	<b>Critères Communs version 3.1 révision 3</b>
Niveau d'évaluation	<b>EAL 4 augmenté ALC_FLR.2</b>
Développeur	<b>PrimeKey Solutions AB</b> Anderstorpsvägen 16, 171 54 Solna, Suède
Commanditaire	<b>PrimeKey Solutions AB</b> Anderstorpsvägen 16, 171 54 Solna, Suède
Centre d'évaluation	<b>Oppida</b> 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables	<div style="display: flex; justify-content: space-around; align-items: center;"><div style="text-align: center;"><b>CCRA</b> </div><div style="text-align: center;"><b>SOG-IS</b> </div></div> <p style="text-align: center;"><b>Le produit est reconnu au niveau EAL4.</b></p>

## Préface

### La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet [www.ssi.gouv.fr](http://www.ssi.gouv.fr).



# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Identification du produit</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	6
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Cycle de vie</i> .....	7
1.2.5. <i>Configuration évaluée</i> .....	8
<b>2. L’EVALUATION .....</b>	<b>9</b>
2.1. REFERENTIELS D’EVALUATION .....	9
2.2. TRAVAUX D’EVALUATION .....	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	9
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	9
<b>3. LA CERTIFICATION .....</b>	<b>10</b>
3.1. CONCLUSION .....	10
3.2. RESTRICTIONS D’USAGE.....	10
3.3. RECONNAISSANCE DU CERTIFICAT .....	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	11
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>12</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>13</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>14</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est l'application « EJBCA version 5.0.4 » développée par PrimeKey Solutions SA.

Ce produit est une suite logicielle qui permet de mettre en œuvre une infrastructure de gestion de clés publiques (ICP ou PKI pour *Public Key Infrastructure*). Il fournit une solution de gestion des certificats (demande, création, renouvellement, révocation), qu'il s'agisse des certificats de chiffrement, d'authentification ou de signature, et une gestion des listes de révocation. Le produit permet de définir une autorité de certification racine, des autorités de certification subalternes et des autorités d'enregistrement.

## 1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP-CIMC] (*Security Level 3*). Cette conformité est de type démontrable.

### 1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par la commande `svn log` à partir des fichiers de code source fournis par le développeur dans un dépôt *subversion* (svn) et téléchargeable en https sur le serveur disponible sur le site [www.ejbca.org](https://www.ejbca.org) (section « *Certified Product for Customers* »).

La réponse attendue à la commande `svn log --stop-on-copy` est : « EJBCA\_5\_0\_4-20120308 ».

Note : Bien qu'une version packagée de EJBCA soit disponible sur le serveur, il est rappelé ici que seule la version non compilée, disponible via le tunnel https à partir du dépôt svn officiel EJBCA, a fait l'objet de l'évaluation.

### 1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la gestion des profils utilisateurs de EJBCA (authentification et contrôle d'accès) ;
- la création de certificats numériques conformes aux standards X.509 v3 et CVC BSI TR-03110 ;
- la création de liste de révocation de certificats ;
- la publication de certificats et de listes de révocation de certificats ;
- le traitement de requêtes OCSP<sup>1</sup> (analyse, réponse) ;

---

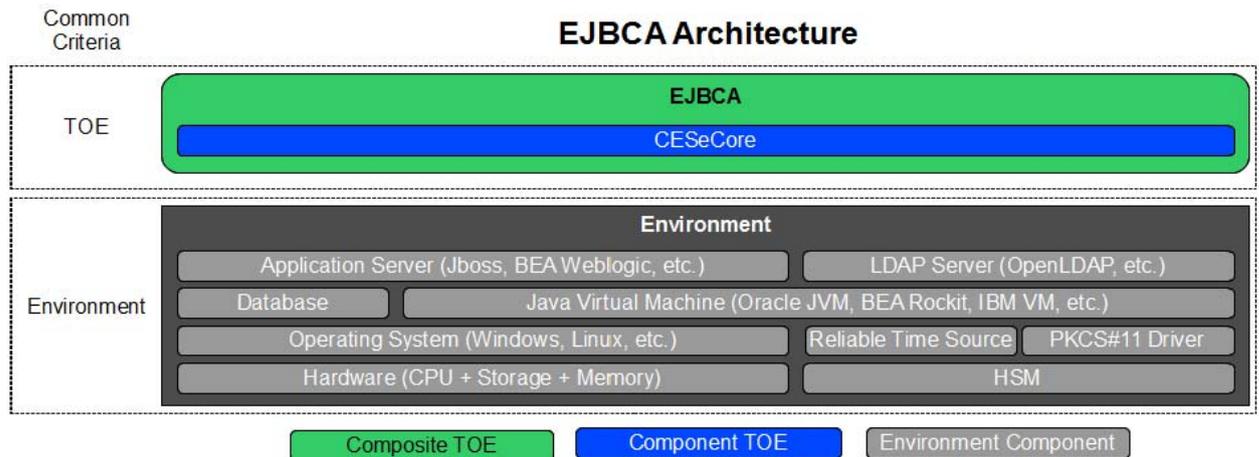
<sup>1</sup> *Online Certificate Status Protocol*.

- le recouvrement de clés ;
- la gestion de *Tokens*, supports de clés privées ;
- la sauvegarde de données de l'application (en vue de leur restauration).

Ces services de sécurité sont détaillés dans la cible de sécurité mais aussi dans le profil de protection [PP-CIMC] d'où ils sont extraits.

### 1.2.3. Architecture

La figure suivante décrit l'architecture du produit dans son environnement :



Le produit intègre la bibliothèque CESeCore, dans sa version v1.1.2, certifiée sous la référence [2012/33].

L'application EJBCA est principalement composée de sept sous-systèmes qui correspondent à ses principales fonctionnalités :

- *Backup & Recovery* : sauvegarde et restauration ;
- *Certificate and Profile Management* : gestion des certificats et des profils ;
- *Security Audit* : audit de sécurité ;
- *Key Management* : gestion des clés ;
- *Identification and Authentication* : identification et authentification ;
- *Access Control* : contrôle d'accès ;
- *Roles* : rôles.

### 1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement est réalisé par la communauté open source « *EJBCA Community* ». Tout contributeur, quelle que soit sa fonction, doit être authentifié pour déposer des modifications ou pour valider le code source ;
- la livraison correspond à la mise à disposition de la version validée dans le dépôt *subversion* sur le serveur de la société PrimeKey hébergé par Office IT Partner ;
- l'installation correspond à la compilation par un utilisateur et à son installation sur un serveur d'application.

Le produit est disponible sur le site audité suivant :

**PrimeKey SA**  
 Chez Office IT Partner  
 Anderstorpsvägen 16,  
 17154 Solna  
 Suède

L'application EJBCA prend en compte les rôles suivants présents dans [PP-CIMC]. Leurs configurations sont décrites dans le guide *Access Control Matrix* référencé dans [GUIDES] :

- l'administrateur qui est en charge de l'installation, de la configuration et de la maintenance de l'application EJBCA ;
- l'auditeur qui est en charge de la consultation et de la maintenance des journaux d'audit ;
- l'officier de sécurité qui est chargé de l'approbation des demandes de génération de certificat ainsi que de leurs révocations ;
- l'opérateur qui est en charge des opérations de sauvegarde et de restauration.

### 1.2.5. Configuration évaluée

Le produit a été testé par le CESTI sur les deux plateformes décrites dans le tableau suivant :

	Plateforme de test n°1 (64 bits)	Plateforme de test n°2 (32 bits)
Système d'exploitation	Red Hat Enterprise Linux v5.5 x86_64	Windows Server 2008 Enterprise with SP2 x86
JDK (Java Développement Kit)	Oracle JDK 1.6.0_27	Oracle JDK1.6.0_24
Base de données	PostgreSQL 9.0.2	MySQL Community server 5.1.55 MySQL Connector/J 5.1.15
Serveur d'application	JBoss 5.1.0.GA	Glassfish v2.1.1
HSM	Safenet LunaSA Version du firmware : 4.6.8	Utimaco CryptoServer Version du firmware : 2.30.2

## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

### 2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 juillet 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

### 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA\_VAN visé.

### 2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

## 3. La certification

### 3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « EJBCA version 5.0.4 », soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant ALC\_FLR.2

### 3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- l'installation des serveurs d'application JBoss ou Glassfish doit être réalisée conformément aux recommandations décrites respectivement dans les guides accessibles aux adresses suivantes :
  - o <http://www.ejbca.org/security.html/#Securing%20JBoss> ;
  - o [http://weblogs.java.net/blog/kalali/archive/2007/12/how\\_to\\_secure\\_g\\_1.html](http://weblogs.java.net/blog/kalali/archive/2007/12/how_to_secure_g_1.html) ;
- les binaires JAR/EAR générés doivent être signés comme précisé dans le document accessibles à l'adresse : <http://ejbca.org/adminguide.html#Code%20signing> ;
- l'accès aux entrées de la base de données, aux journaux et aux binaires (dont les fichiers de configuration) doit être strictement réservé à des personnels de confiance.

### 3.3. Reconnaissance du certificat

#### 3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord<sup>1</sup>, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



#### 3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires<sup>2</sup>, des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC\_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



---

<sup>1</sup> Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

<sup>2</sup> Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

## Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	1	Identification of security measures
	ALC_FLR								2	2	Flaw reporting procedures
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	3	3	Focused vulnerability analysis

## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- « Security Target for EJBCA v5.0.4 », référence D10.0, version 1.2, 2 juillet 2012.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- « Evaluation Technical Report - EJBCA version 5.0.4 », référence OPPIDA/CESTI/EJBCA/RTE , version 1.1, 6 juillet 2012.</li> </ul>
[CONF]	<p><a href="https://www.wiki.cesecore.eu/index.php/Main_Page">https://www.wiki.cesecore.eu/index.php/Main_Page</a> partie EJBCA 5.0.4 - Configuration List (internal Development) et Configuration List (External Libs).</p>
[GUIDES]	<p><a href="https://www.wiki.cesecore.eu/index.php/Main_Page">https://www.wiki.cesecore.eu/index.php/Main_Page</a> partie EJBCA 5.0.4 - Preparative Procedure (AGD_PRE) et Operational User Guidance (AGD_OPE) :</p> <ul style="list-style-type: none"> <li>- dont Access Control Matrix, version 1.2, 16 décembre 2011.</li> </ul>
[PP-CIMC]	<p>Certificate Issuing and Management Components – Family of Protection Profiles, version 1.0, 31 octobre 2001. <i>Certifié par le NIST (National Institute of Standards and Technology) sous la référence CCEVS-VR-01-0009.</i></p>
[2012/33]	<p>CESeCore, version 1.1.2. <i>Certifié par l'ANSSI sous la référence ANSSI-CC- 2012/33.</i></p>

### Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .  Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .