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-2012/33

CESeCore version 1.1.2

Paris, le 14 Juin 2012

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

[ORIGINAL SIGNE]

Patrick Pailloux

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 présupposées 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

Référence du rapport de certification

ANSSI-CC-2012/33

Nom du produit

CESeCore version 1.1.2

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_FLR.2

Développeur

CESeCore Consortium

www.cesecore.eu

Commanditaire

CESeCore Consortium

www.cesecore.eu

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Accords de reconnaissance applicables

CCRA

Le produit est reconnu au niveau EAL4.

SOG-IS

Le produit est reconnu au niveau EAL4.

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.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la librairie open source « CESeCore version 1.1.2 » développée par le consortium CESeCore.

Ce produit est composé de modules logiciels JEE (*Java Enterprise Edition*) offrant des fonctions de sécurité nécessaires à la création d'applications basées sur une *PKI*[1].
La librairie CESeCore n'est pas une application en elle-même car elle doit être intégrée dans une application de type JEE et déployée sur un serveur d'applications afin de fournir les fonctions de sécurité attendues par les applications tierces.
Chaque fonction de sécurité implémentée est atteinte via des API[2] (au choix des API Java ou des API spécifiques JEE). En dehors de fonctions de sécurité, CESeCore ne fournit pas de fonctionnalités de haut-niveau : elles devront être implémentées dans des applications tierces. Ces applications intégrant CESeCore et son environnement dont, par exemple, les accès aux ressources cryptographiques peuvent être des applications de gestion de certificats, des serveurs d'horodatage, des répondeurs OCSP[3], des solutions de signature de documents ou des serveurs d'archives sécurisées.

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 basée sur le profil de protection [PP-CIMC] (*Security Level 3*).
Toutes les hypothèses, menaces, politiques, exigences de sécurité et tous les objectifs définis dans le [PP-CIMC] ont été reproduits dans la cible de sécurité en les adaptant aux CC v3.1.

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 téléchargé en https sur le serveur disponible sur le site officiel www.cesesecore.eu.
La réponse attendue à la commande *svn log --stop-on-copy* est : CESeCore_1_1_2-20111017.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- la journalisation (audit) de sécurité ;
- la gestion des rôles ;
- la sauvegarde et la restauration ;

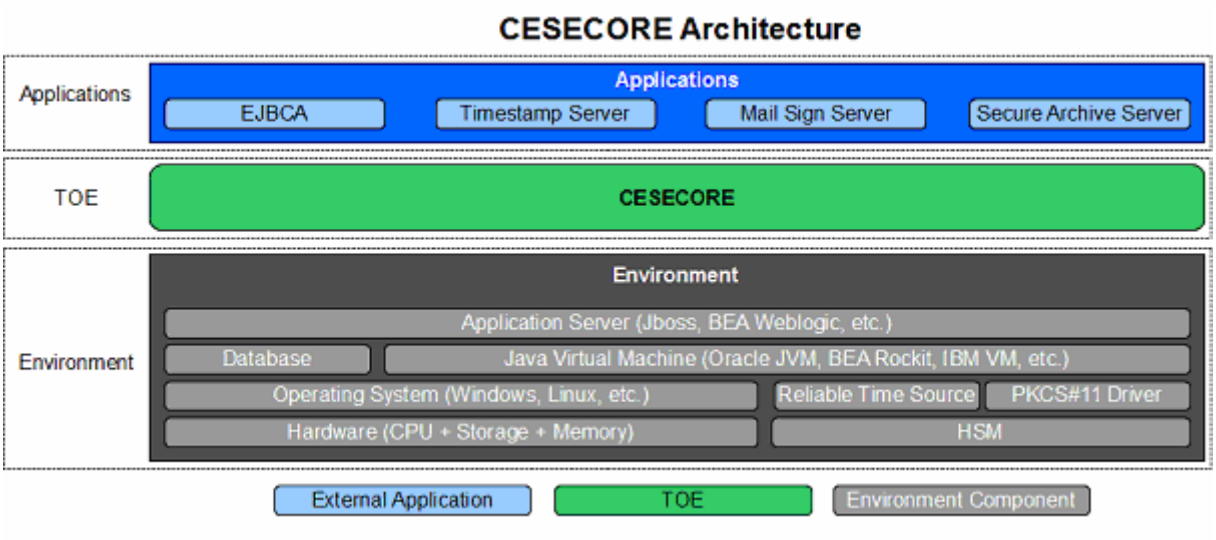
[1] *Public Key Infrastructure* ou IGC pour Infrastructure de Gestion de Clés.
[2] *Application Programming Interface.*
[3] *Online Certificate Status Protocol.*

- le contrôle d'accès ;
- l'identification et l'authentification ;
- l'export et l'import de données distantes ;
- la gestion des clés ;
- la gestion des profils et des certificats.

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

L'architecture de fonctionnement de CESeCore peut être décrite comme ci-dessous :



La TOE est principalement composée de huit 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 ;
- *Access Control* : contrôle d'accès ;
- *Roles* : rôles ;
- *Identification and Authentication* : identification et authentification ;
- *Trusted Time* : horloge de confiance.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement est réalisé par la communauté open source « Consortium CESeCore». 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, à son installation sur un serveur d'application et/ou à son intégration dans une application.

Le produit est disponible sur le site audité suivant :

PrimeKey SA

Chez Office IT Partner
Anderstorpsvagen 16,
17154 Solna
Suède

Les applications qui intégreront la TOE devront considérer 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 ;
- l'auditeur qui est en charge de consulter et maintenir les journaux d'audit ;
- « l'officier » qui est en charge des demandes, des approbations et de révocations des certificats ;
- l'opérateur qui est en charge des opérations de sauvegarde et de restauration.

1.2.5. Configuration évaluée

Le certificat porte sur la librairie CESeCore 1.1.2 dont le label complet est CESeCore_1_2-20111017 tel que décrit au 1.2.1.
Le certificat porte sur les deux environnements suivants combinant des produits open source et commerciaux :

Item	Platform A	Platform B
OS	Red Hat Enterprise Linux v5.5 x86_64 (64bit)	Windows Server 2008 Enterprise with SP2 x86 (32bit)
JDK	Oracle JDK 1.6.0_20 64 bit	Oracle JDK 1.6.0_23 32 bit
Database	PostgreSQL 9.0.2	MySQL Community Server 5.1.55 MySQL Connector/J 5.1.15
Application Server	JBoss 5.1.0.GA	Glassfish v2.1.1
HSM	Safenet LunaSA Firmware version 4.6.8	Utimaco CryptoServer Firmware version 2.30.2

Note importante : même si une version packagée de CESeCore est 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 CESeCore, a fait l'objet de l'évaluation.

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 1 juin 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 « CESeCore version 1.1.2 », soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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 :

- les installations des serveurs d'application JBoss ou Glassfish doivent être sécurisés via la mise en œuvre des guides adéquats https://wiki.cesecore.eu/mediawiki/index.php/JBoss#securing_the_installation pour JBoss ou https://wiki.cesecore.eu/mediawiki/index.php/Glassfish#securing_the_installation pour Glassfish ;
- les binaires JAR/EAR générés doivent être signés comme précisé dans le document suivant (http://ejbca.org/adminguide.html#Code%20signing) ;
- les accès aux entrées de la base de données, aux journaux et aux binaires (dont les fichiers de configuration) doivent être strictement réservés aux 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[1], 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[2], 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 :

[1] 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.

[2] 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**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic Modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**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**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**2**	Flaw reporting procedures
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing - sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target for CESeCore v1.1.2, version 1.1, date, CESeCore Consortium.*
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report CESeCore project, reference OPPIDA/CESTI/CESECORE/RTE/1.2 du 1/06/2012 – v1.2 – 1st june 2012, OPPIDA.*
[CONF]	https://www.cesecore.eu/mediawiki/index.php/Main_Page partie CESeCore 1.1.2 - *Configuration List (internal Development)* et *Configuration List (External Libs).*
[GUIDES]	https://www.cesecore.eu/mediawiki/index.php/Main_Page partie CESeCore 1.1.2 - *Preparative Procedure (AGD_PRE)* et *Operational User Guidance (AGD_OPE).* dont *Access Control Matrix - version 1.6 – 26th november 2011.*
[PP-CIMC]	*Protection Profile, Certificate Issuing and Management Components Family of Protection Profiles, Version 1.0 October 31, 2001.* Certifié par le NIAP *(National Information Assurance Partnership).*

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 www.ssi.gouv.fr.
	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 www.ssi.gouv.fr.