PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2009/16

Logiciel OpenTrust PKI version 4.3.4

Paris, le 7 juillet 2009

Le Directeur central 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 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 la direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification **DCSSI-2009/16**
Nom du produit **Logiciel OpenTrust PKI**
Référence/version du produit **Version 4.3.4**
Conformité à un profil de protection **Certificate Issuing and Management Components (CIMCs) Security Level 2 Protection Profile**
Critères d'évaluation et version **Critères Communs version 3.1**
Niveau d'évaluation **EAL 3 augmenté** **ALC_CMS.4, ALC_FLR.2**
Développeur(s) **OpenTrust SA** **20 rue Rouget de Lisle, 92130 Issy Les Moulineaux, France**
Commanditaire **OpenTrust SA** **20 rue Rouget de Lisle, 92130 Issy Les Moulineaux, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France** **Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr**
Accords de reconnaissance applicables **CCRA** **SOG-IS**

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 n° 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 le « Logiciel OpenTrust PKI**,** Version 4.3.4 **»** développé par OpenTrust SA.

Ce produit est une suite logicielle qui permet de mettre en œuvre une infrastructure à clé publique (ICP ou PKI pour *Public Key Infrastructure*). Il peut être utilisé pour mettre en œuvre une grande variété d'infrastructures, de la plus simple à la plus complexe. Il fournit une solution de gestion des certificats (demande, création, renouvellement, révocation), que ce soit 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. Elle est conforme au niveau de sécurité 2 du profil de protection « Certificate Issuing and Management Components » [PP CIMC].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version 4.3.4 certifiée du produit OpenTrust PKI est identifiable par le label figurant sur le CD-ROM.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la collecte des données d'audit, la possibilité de lire les journaux d'audit et la restriction de l'accès aux journaux d'audit (*Security Audit*) ;
- la traçabilité des actions réalisées sur un certificat (création, révocation, suppression), des tentatives d'authentification et des modifications effectuées sur les rôles et droits d'accès d'un utilisateur (*Security Audit*) ;
- l'implémentation des rôles « administrateur » et « officier » tels que spécifiés dans le profil de protection [PP CIMC] au niveau de sécurité 2 (*Roles*) ;
- une fonctionnalité de sauvegarde configurable et des fonctions de restauration du système (*Backup and Recovery*) ;
- le maintien d'une base de données sécurisée des opérateurs autorisés, incluant toutes les identités et les autorisations (*Access Control*) ainsi que toutes les informations sur les certificats et les rôles qui peuvent être affectés (*Identification and Authentication*) ;
- des mécanismes permettant de sécuriser l'import et l'export de données distantes dans un environnement ou un réseau non sûr (*Remote Data Entry and Export*) ;
- la gestion des clés (*Key Management*) ;
- la gestion des certificats et des listes de révocation (*Certificate Management*).

1.2.3. Architecture

Le produit est constitué des modules habituels d'une infrastructure à clé publique : une autorité de certification racine, des autorités de certification subalternes, des autorités d'enregistrement et des entités d'enrôlement tels que définis dans le profil de protection [PP CIMC].

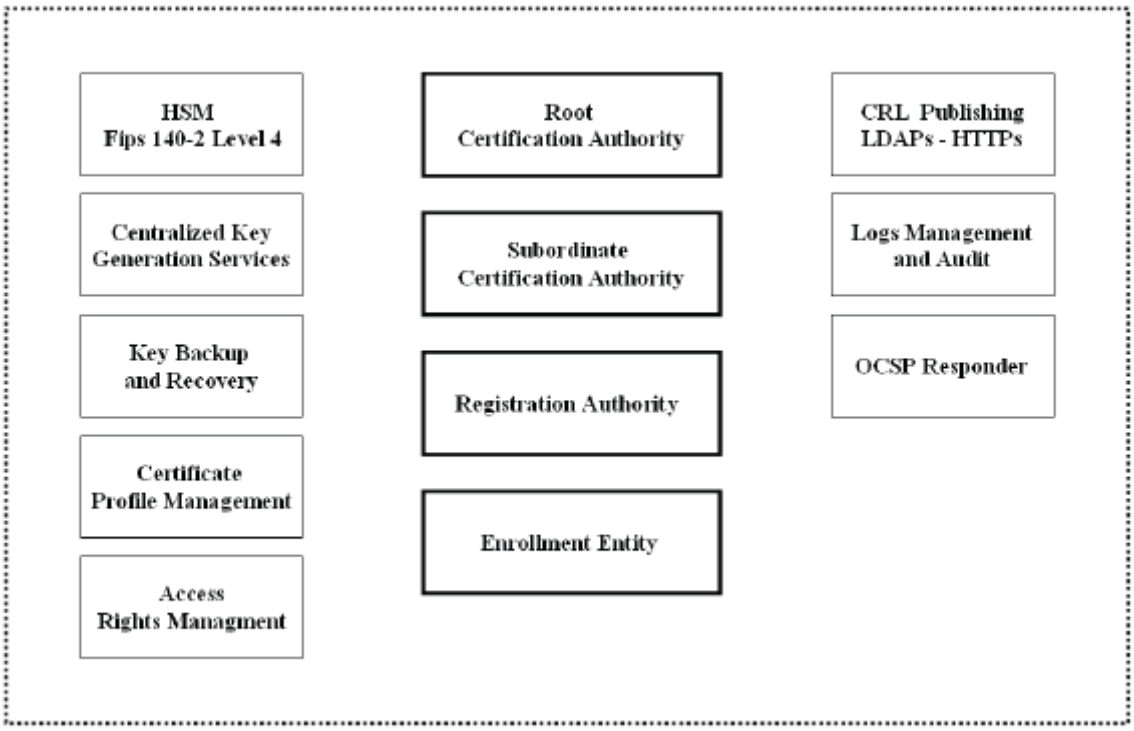

Figure 1 - Périmètre logique de la TOE

Les modules (entité d'enrôlement, autorité d'enregistrement, autorité de certification) peuvent être déployés sur une seule machine ou sur plusieurs machines en fonction de l'architecture de déploiement du client.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés par OpenTrust SA ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

OpenTrust SA

15/17 avenue de Ségur
75007 Paris
France

Le produit peut être livré sur un CD-ROM et dans une image ISO. Lors de la réception du produit, le client doit s'assurer de l'intégrité de la TOE en vérifiant l'empreinte SHA1 de l'image ISO et des fichiers si la livraison a été faite sur un CD-ROM. L'empreinte servant de

base pour la comparaison est délivrée dans un fichier (integrity.txt). L'authentification des fichiers d'intégrité (SHA1SUM et integrity.txt) est vérifiée en utilisant une signature PGP.

Les administrateurs du produit sont les « Administrateurs » et les « Officiers » tels que spécifiés dans le profil de protection [PP CIMC] au niveau de sécurité 2. Dans le cadre de cette évaluation, les rôles « Opérateur » et « Auditeur » sont associés au rôle « Administrateur ».

Les utilisateurs du produit sont des personnes ou des processus opérant pour le compte de la personne, et qui accèdent au système de gestion des certificats.

1.2.5. Configuration évaluée

Le modèle d'architecture choisi pour l'évaluation est celui du déploiement des modules sur une seule machine.

Le produit a été évalué sur la configuration suivante :

- modèle de la machine : HP ProLiant DL360 G3 ;
- système d'exploitation : SUSE Linux Enterprise Server 10 SP1 ;
- boîtier HSM : nCipher nShield PCI.

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 4 juin 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

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 n° 2002-535.

Ce certificat atteste que le produit « Logiciel OpenTrust PKI, Version 4.3.4 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- identifier et surveiller les événements liés à la sécurité en faisant en sorte que les auditeurs lisent les journaux d'audit à une fréquence en rapport avec le niveau de risque (O.Auditors Review Audit Logs) ;
- s'assurer, à travers la mise en œuvre d'une gestion des données d'authentification, que les utilisateurs changent régulièrement et de façon appropriée leurs données d'authentification (note : cet objectif n'est pas applicable aux données d'authentification biométriques) (O.Authentication Data Management) ;
- assurer une protection physique des moyens de communication utilisés par la TOE (O.Communications Protection) et des composants de la TOE (O.Physical Protection) ;
- avoir une gestion efficace de la TOE en confiant à des administrateurs, des opérateurs, des officiers et des auditeurs compétents la gestion de la TOE et la sécurité des informations qu'elle contient (O.Competent Administrators, Operators, Officers and Auditors) ;
- faire en sorte que tous les administrateurs, opérateurs, officiers et auditeurs soient familiers avec la politique de certification (PC) et la déclaration des pratiques de certification (DPC) sous lesquelles la TOE est exploitée (O.CPS) ;
- détruire de manière appropriée les données d'authentification et les privilèges associés après qu'un accès ait été supprimé (par exemple suite à une fin de contrat ou à un changement de responsabilité) (O.Disposal of Authentication Data) ;
- notifier les autorités compétentes de tous les problèmes de sécurité qui pourraient impacter leurs systèmes pour minimiser les risques de perte ou de compromission de données (O.Notify Authorities of Security Issues) ;
- délivrer une formation aux utilisateurs, administrateurs, opérateurs, officiers et auditeurs aux techniques permettant de contrer les attaques par ingénierie sociale (O.Social Engineering Training) ;

- s'assurer que les utilisateurs acceptent d'accomplir des tâches ou un groupe de tâches qui demandent un environnement des technologies de l'information sûr et des informations gérées par la TOE (O.Cooperative Users) ;
- les administrateurs, opérateurs, officiers et auditeurs doivent être de confiance (O.No Abusive Administrators, Operators, Officers and Auditors) et doivent réaliser leurs tâches sur des postes de travail sûrs pour éviter que quelqu'un se fasse passer pour eux ;
- mettre en œuvre l'infrastructure conformément à une politique de certification (PC) et à sa déclaration des pratiques de certification (DPC) associée ; en particulier, les profils des certificats et les règles de nommage doivent être clairement définis dans ces documents ;
- au niveau de l'environnement réseau, restreindre les flux entrants aux seuls protocoles exigés : http/https et ssh, si celui-ci est nécessaire pour l'administration du système à distance.

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 1999 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 E6 et CC EAL7. 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'Espagne, la Finlande, la France, la Grèce, 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, la République de Corée, le Pakistan, les Pays-Bas, 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 3+	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**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	**2**		
	ADV_INT					**2**	**3**	**3**		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural 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	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ADO_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		
ASE Security Target Evaluation	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**	2	**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	**2**	Vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - OpenTrust PKI v4 Security Target, Référence : pki-cc-st, version 2.2 révision 96095 du 03/06/2009 OpenTrust SA
[RTE]	Rapport technique d'évaluation – Projet OTTAWA Référence : OPPIDA/CESTI/OTTAWA/RTE/1 du 04/06/2009 OPPIDA
[CONF]	Liste de configuration de la version 4.3.4 Référence : TOE_Configuration_List 4.3.4, version 4.3.4 du 26/05/2009 OpenTrust SA
[GUIDES]	Guide d'installation du produit : - Guideline for OpenTrust PKI installation Référence : pki-cc-installation-guideline-eng, révision 90743 du 03/02/2009 OpenTrust SA - OpenTrust PKI 4.3 Installation Guide Référence : pki-install-guide-eng, révision 94705 du 29/04/2009 OpenTrust SA - Ncipher PCI and Additional Security Packages Installation Guide Référence : pki-cc-ncipher-security-eng, révision 95025 du 05/05/2009 OpenTrust SA Guide d'administration du produit : - OpenTrust PKI 4.3 Administrator Guide Référence : pki-admin-guide-eng, révision 95148 du 07/05/2009 OpenTrust SA - OpenTrust PKI log database Référence : pki-audit-logs-eng, révision 92778 du 17/03/2009 OpenTrust SA - nShield User Guide, version 6.2 du 08/07/2008 [IN.050] nCipher Guide d'utilisation du produit : - OpenTrust PKI 4.3 Registration Authority Officer's Guide Référence: pki-rao-guide-eng, révision 90743 du 03/02/2009 OpenTrust SA - OpenTrust PKI 4.3 Registration Authority Manager's Guide Référence: pki-ram-guide-eng, révision 95673 du 25/05/2009 OpenTrust SA

[PP CIMC]	Certificate Issuing and Management Components – Family of Protection Profiles, version 1.0 du 31 octobre 2001. *Certifié par le NIST (National Institute of Standards and Technology) sous la référence CCEVS-VR-01-0009.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[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 2.0, April 1999, Management Committee of Agreement Group.