



PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2009/16

OpenTrust PKI software, version 4.3.4

Paris, 7th of July 2009

Courtesy Translation



Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.

Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.



Any correspondence about this report has to be addressed to:

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
France

certification.dcssi@sgdn.gouv.fr

Reproduction of this document without any change or cut is authorised.



<i>Certification report reference</i>	DCSSI-2009/16
<i>Product name</i>	OpenTrust PKI software
<i>Product reference</i>	Version 4.3.4
<i>Protection profile conformity</i>	Certificate Issuing and Management Components (CIMCs) Security Level 2 Protection Profile
<i>Evaluation criteria and version</i>	Common Criteria version 3.1
<i>Evaluation level</i>	EAL 3 augmented ALC_CMS.4, ALC_FLR.2
<i>Developer(s)</i>	OpenTrust SA 20 rue Rouget de Lisle, 92130 Issy Les Moulineaux, France
<i>Sponsor</i>	OpenTrust SA 20 rue Rouget de Lisle, 92130 Issy Les Moulineaux, France
<i>Evaluation facility</i>	Oppida 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France Phone: +33 (0)1 30 14 19 00, email : cesti@oppida.fr
<i>Recognition arrangements</i>	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div>

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.



Content

1. THE PRODUCT	6
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION	6
1.2.1. <i>Product identification</i>	6
1.2.2. <i>Security services</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Life cycle</i>	7
1.2.5. <i>Evaluated configuration</i>	8
2. THE EVALUATION.....	9
2.1. EVALUATION REFERENTIAL	9
2.2. EVALUATION WORK	9
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	9
3. CERTIFICATION.....	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS	10
3.3. RECOGNITION OF THE CERTIFICATE	11
3.3.1. <i>European recognition (SOG-IS)</i>	11
3.3.2. <i>International common criteria recognition (CCRA)</i>	11
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....	12
ANNEX 2. EVALUATED PRODUCT REFERENCES	13
ANNEX 3. CERTIFICATION REFERENCES	15

1. The product

1.1. Presentation of the product

The evaluated product is “OpenTrust PKI software, Version 4.3.4” developed by OpenTrust SA.

This product is a software suite for implementing a Public Key Infrastructure (PKI). It can be used to implement a wide variety of infrastructures, from the most basic to the most structurally complex. It includes a solution for certificate management (request, creation, renewal, revocation), for encryption, authentication and signature certificates, as well as revocation list management. It can be used to define a Root Certification Authority, Subordinate Certification Authorities and Registration Authorities.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

This security target is compliant to the security level 2 of the « Certificate Issuing and Management Components » Protection Profile [PP CIMC].

1.2.1. Product identification

The configuration list [CONF] identifies the product’s constituent elements.

The certified version 4.3.4 of the OpenTrust PKI software can be identified using the label on the CD-ROM.

1.2.2. Security services

The principal security services provide by the product are:

- the collection of audit data, the ability to review audit logs and to restrict access to audit logs (*Security Audit*);
- the tracking of any actions taken to a certificate (creation, revocation, deletion), of authentication attempts and of any changes made to user’s roles and access rights (*Security Audit*);
- the implementation of Administrator and Officer roles as specified in the Protection Profile [PP CIMC] at the security level 2 (*Roles*);
- the configurable backup functionality and system recovery features (*Backup and Recovery*);
- the maintenance of a secure data base of authorized operators, including all identities and permissions (*Access Control*) as well as all certificates information and roles that can be granted (*Identification and Authentication*);
- the mechanisms to secure remote data entry and export over an untrusted exchange environment or network (*Remote Data Entry and Export*);
- key management (*Key management*);
- the management of certificates and revocation lists (*Certificate Management*)

1.2.3. Architecture

The product is composed of classical PKI modules: Root Certification Authority, Subordinate Certification Authorities, Registration Authorities and Enrollment Entities as defined in the Protection Profile [PP CIMC].

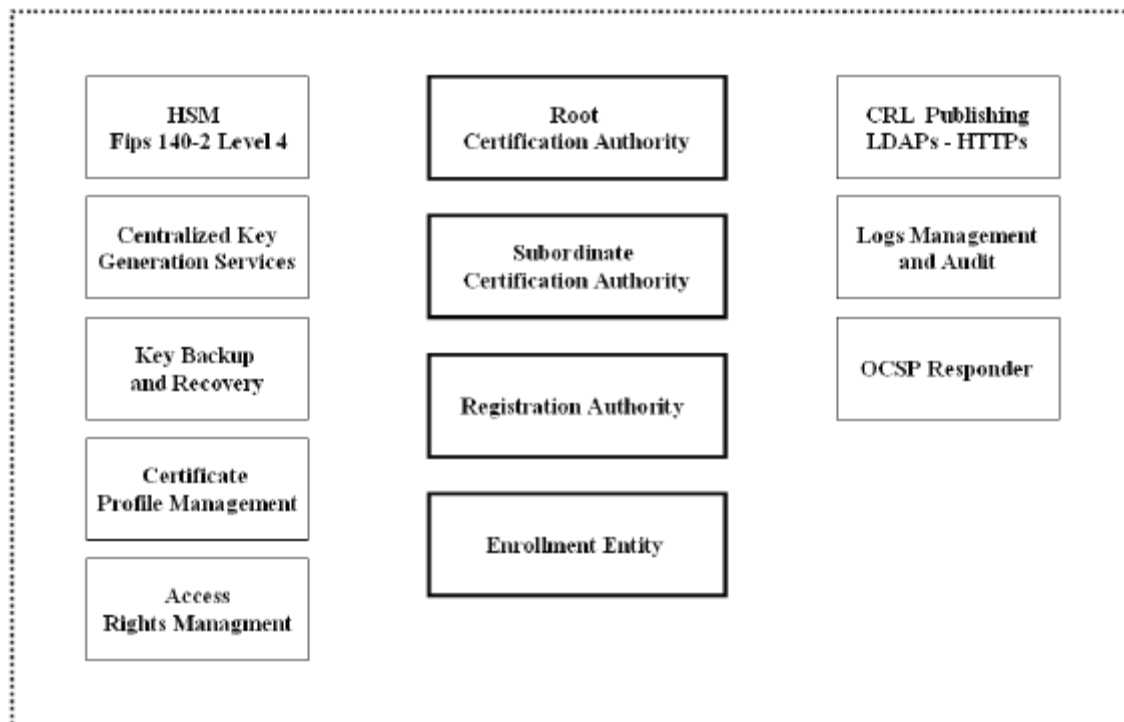


Figure 1 - Logical scope of the TOE

The modules (Enrollment Entity, Registration Authority, Certification Authority) can be deployed on just one machine or several machines according to the client deployment architecture.

1.2.4. Life cycle

The product's life cycle is organized as follows:

- development and delivery of the product are performed by OpenTrust SA;
- installation, administration and use of the product correspond to product deployment, performed by the client.

The product has been developed on the following site:

OpenTrust SA

15/17 avenue de Ségur
75007 Paris
France

The product can be delivered either as a physical CD-Rom or as an ISO image. Upon reception, the client must verify the integrity of the TOE by checking the SHA1 checksum of the ISO image or of the packages if the delivery was made on a CD-ROM. The checksum used for comparison is found in a file (integrity.txt) contained in the delivery. The

authentication of integrity files (SHA1SUM and integrity.txt) is verified using a PGP signature.

The Product Administrators are the “Administrators” and the “Officers” as specified in the Protection Profile [PP CIMC] at the security level 2. For this evaluation, “Operator” and “Auditor” roles are aggregated to the Administrator role.

The Product Users are individuals, or processes associated with individuals, that access the certificate management system.

1.2.5. Evaluated configuration

The architecture model chosen for the evaluation is the one-machine architecture model.

The following configuration was used for the evaluation:

- machine model: HP ProLiant DL360 G3;
- operating system: SUSE Linux Enterprise Server 10 SP1;
- HSM: nCipher nShield PCI.



2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 [CC]** and with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The evaluation technical report [ETR], delivered to DCSSI the 4th of June 2009, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “**pass**”.

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has not been analysed by DCSSI.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product “OpenTrust PKI software, Version 4.3.4” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 3 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- identify and monitor security-relevant events, ensuring that the Auditors review the audit logs periodically appropriate to the level of risk (*O.Auditors Review Audit Logs*);
- ensure that users change their authentication data at appropriate intervals and to appropriate values through enforced authentication data management (note: this objective is not applicable to biometric authentication data) (*O.Authentication Data Management*);
- ensure physical protection of the TOE’s means of communication (*O.Communications Protection*) and security-relevant components (*O. Physical Protection*);
- ensure efficient management of the TOE by entrusting TOE management and the security of the information it contains to competent Administrators, Operators, Officers and Auditors (*O.Competent Administrators, Operators, Officers and Auditors*);
- ensure that all Administrators, Operators, Officers and Auditors are familiar with the Certification Policy (CP) and the Certification Practices Statement (CPS) under which the TOE is operated (*O.CPS*);
- provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility) (*O.Disposal of Authentication Data*);
- notify all competent authorities of any security issues that may impact their systems in order to minimize risks of lost or compromised data (*O.Notify Authorities of Security Issues*);
- provide training for users, Administrators, Operators, Officers and Auditors in techniques to thwart social engineering attacks (*O.Social Engineering Training*);
- ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE (*O.Cooperative Users*);



- use trustworthy Administrators, Operators, Officers and Auditors (*O.No Abusive Administrators, Operators, Officers and Auditors*) who must perform all their tasks on secure workstations so that no doubt exists regarding their identities;
- implement the infrastructure in conformity with a Certification Policy (CP) and its associated Certification Practices Statement (CPS); in particular the certificate profiles and naming rules must be clearly specified in these documents;
- with regards to the network environment, limit entry flows to the required protocols only: http/https and ssh, if this is required for remote system administration.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement¹, of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:



3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries², of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:



1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Name of the component
ADV Development	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 Guidance	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 Life-cycle support	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 Vulnérability assessment	AVA_VAN	1	2	2	3	4	5	5	2	Vulnerability analysis



Annex 2. Evaluated product references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> - OpenTrust PKI v4 Security Target, Reference: pki-cc-st, version 2.2 revision 96095 dated 03/06/2009 OpenTrust SA
[ETR]	<p>Evaluation technical report – OTTAWA project Reference: OPPIDA/CESTI/OTTAWA/RTE/1 dated 04/06/2009 OPPIDA</p>
[CONF]	<p>Configuration list for version 4.3.4 Reference: TOE Configuration List 4.3.4, version 4.3.4 dated 26/05/2009 OpenTrust SA</p>
[GUIDES]	<p>Product installation guide:</p> <ul style="list-style-type: none"> - Guideline for OpenTrust PKI installation Reference: pki-cc-installation-guideline-eng, revision 90743 dated 03/02/2009 OpenTrust SA - OpenTrust PKI 4.3 Installation Guide Reference: pki-install-guide-eng, revision 94705 dated 29/04/2009 OpenTrust SA - Ncipher PCI and Additional Security Packages Installation Guide Reference: pki-cc-ncipher-security-eng, revision 95025 dated 05/05/2009 OpenTrust SA <p>Product administration guide:</p> <ul style="list-style-type: none"> - OpenTrust PKI 4.3 Administrator Guide Reference: pki-admin-guide-eng, revision 95148 dated 07/05/2009 OpenTrust SA - OpenTrust PKI log database Reference: pki-audit-logs-eng, revision 92778 dated 17/03/2009 OpenTrust SA - nShield User Guide, version 6.2 dated 08/07/2008 nCipher <p>Product user guide:</p> <ul style="list-style-type: none"> - OpenTrust PKI 4.3 Registration Authority Officer's Guide Reference: pki-rao-guide-eng, revision 90743 dated 03/02/2009 OpenTrust SA - OpenTrust PKI 4.3 Registration Authority Manager's Guide Reference: pki-ram-guide-eng, revision 95673 dated 25/05/2009 OpenTrust SA



[PP CIMC]	Certificate Issuing and Management Components – Family of Protection Profiles, version 1.0 dated 31/10/2001. <i>Certified by the NIST (National Institute of Standards and Technology), under the reference CCEVS-VR-01-0009.</i>
-----------	--



Annex 3. Certification references

Decree number 2002-535 dated 18 th April, 2002 related to the security evaluations and certifications of information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 Certification of the security provided by IT products and systems, 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, revision 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.