PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/38

ExaProtect Security Management Solution (SMS)

Paris, 27th of November 2008

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

Certification report reference

DCSSI-2008/38

Product name

ExaProtect Security Management Solution (SMS)

Product reference

Version 2.7.3.5

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 2 augmented

ADV_HLD.2, ADV_IMP.1*, ADV_LLD.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1, AVA_VLA.2

***applied to FCS functional requirements**

Developer(s)

ExaProtect

149 boulevard Stalingrad, 69100 Villeurbanne, France

Sponsor

ExaProtect

149 boulevard Stalingrad, 69100 Villeurbanne, France

Evaluation facility

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

Recognition arrangements

CCRA **SOG-IS**

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

1.1. Presentation of the product

The evaluated product is « ExaProtect Security Management Solution (SMS)**,** Version 2.7.3.5 » developed by ExaProtect.

The ExaProtect SMS product enables to answer to the security supervision needs. These needs can be summarize as follows:

- to manage a high number of security devices divided on the whole information system;
- to process the lot of information generated by the devices;
- to improve the events (reduction of false positives, take into account of the "trade" context);
- to correlate the events coming from different devices and to generate alerts;
- to automate the diagnosis process;
- to call attention to the human expertise on the most important threat;
- to propose counter measures when it is possible;
- to provide a synthetic and global view on the risk and on the threat.

These services are realized by the two main components ExaProtect Security Management Agent (**SMA**) and ExaProtect Security Management Platform (**SMP**). The security events analysis and the solution configuration are realized via the ExaProtect Security Management Console (**SMC**) from a work station with a Web browser.

1.2. Evaluated product description

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

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.
The certified version of the product can be identified by the following elements:

- version: 2.7.3.5;
- build number: 390;
- commit number: 16754.

This information is available via the window « About » of the SMC console.
The version number of the product is also indicated on the SMC console home page.

The installed agents' version is available on the file *version* which is in the *ExaProtect Technology\ESMA 2.7.3.3\config* directory on the work station where the agent is installed.

1.2.2. Security services

The product mainly provides the following security services:

- identification and authentication of users who connect to the ExaProtect SMS product console in order to manage alerts;
- users profiles management and rights agreement according to a rights table;
- protection and access control to the server configuration files;
- protection and access control to the tables of the server data-bases;
- collection of equipment events and raw logs as well as internal ones within the agent operation;
- collection of internal events in the SMP server operation;
- audit of collected events at agents and SMP server level;
- synchronization of the agents' configuration at startup and also at an authorized user request;
- prevention of a breaking link with the agent;
- confidentiality and integrity of exchanges between the server and its agents;
- confidentiality and integrity of exchanges between the console and the server;
- confidentiality and integrity of raw log archiving.

1.2.3. Architecture

The figure below presents a global view of the ExaProtect SMS concept and the services provided by the product:

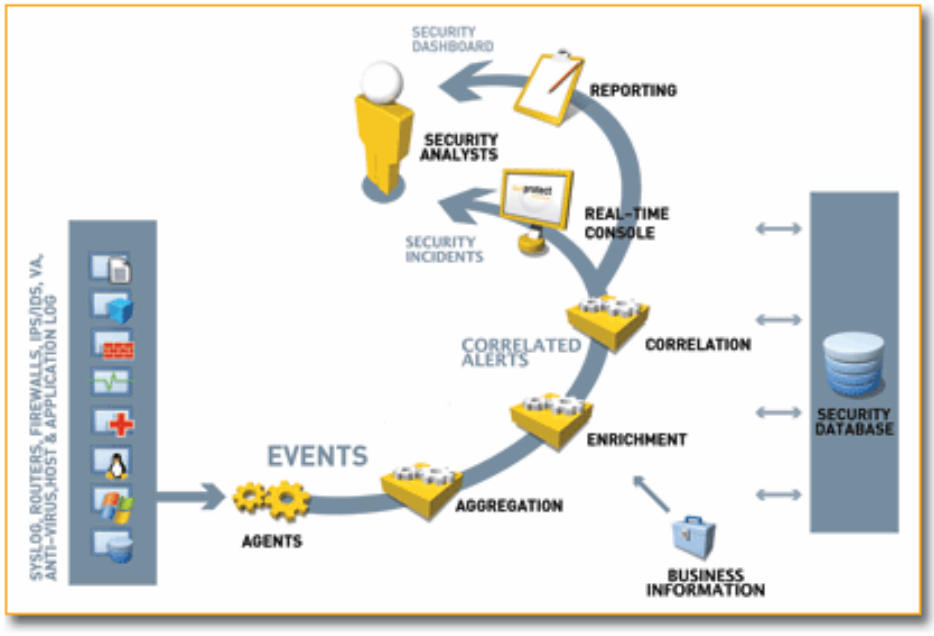

Figure 1 - TOE use cases

The scheme below presents the evaluation scope associated to the product components:

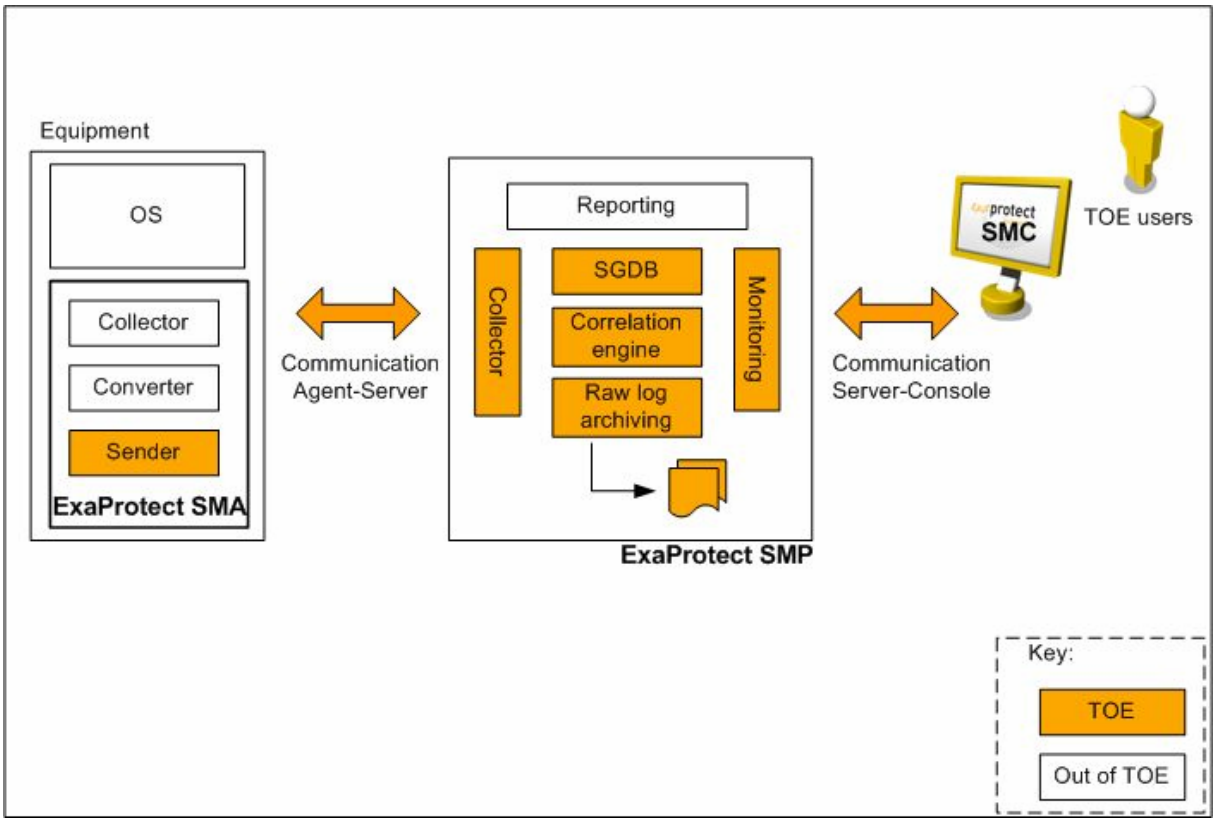

Figure 2 - TOE architecture

SGDB in the figure above corresponds to the data bases management system.

The evaluation scope is the following one:

- the collection of events and raw logs by the SMP server sent by the SMA agent;
- the application of events' correlation rules in order to generate security alerts;
- the security alerts analysis through audit functions accessible via the SMC console;
- the communications between agents and the server;
- the communications between the console and the server, including the users authentication mechanism and the access control;
- the archiving of raw logs coming from equipment units.

The following elements are out of the scope of the evaluation:

- the "reporting" mechanisms from events and security alerts stored in the data base;
- the collection of log entries on the equipment, their communication toward an agent and their tranformation into events and raw logs;
- the relevance of rules and heuristics used par the correlation engine to manage the alerts.

1.2.4. Life cycle

The product has been developed on the following site:

ExaProtect Innovation

149 boulevard Stalingrad
69100 Villeurbanne
France

The equipment and certificates delivery process is described in the figure bellow. The certificate enables a customer to download patches, updates and product documentation.

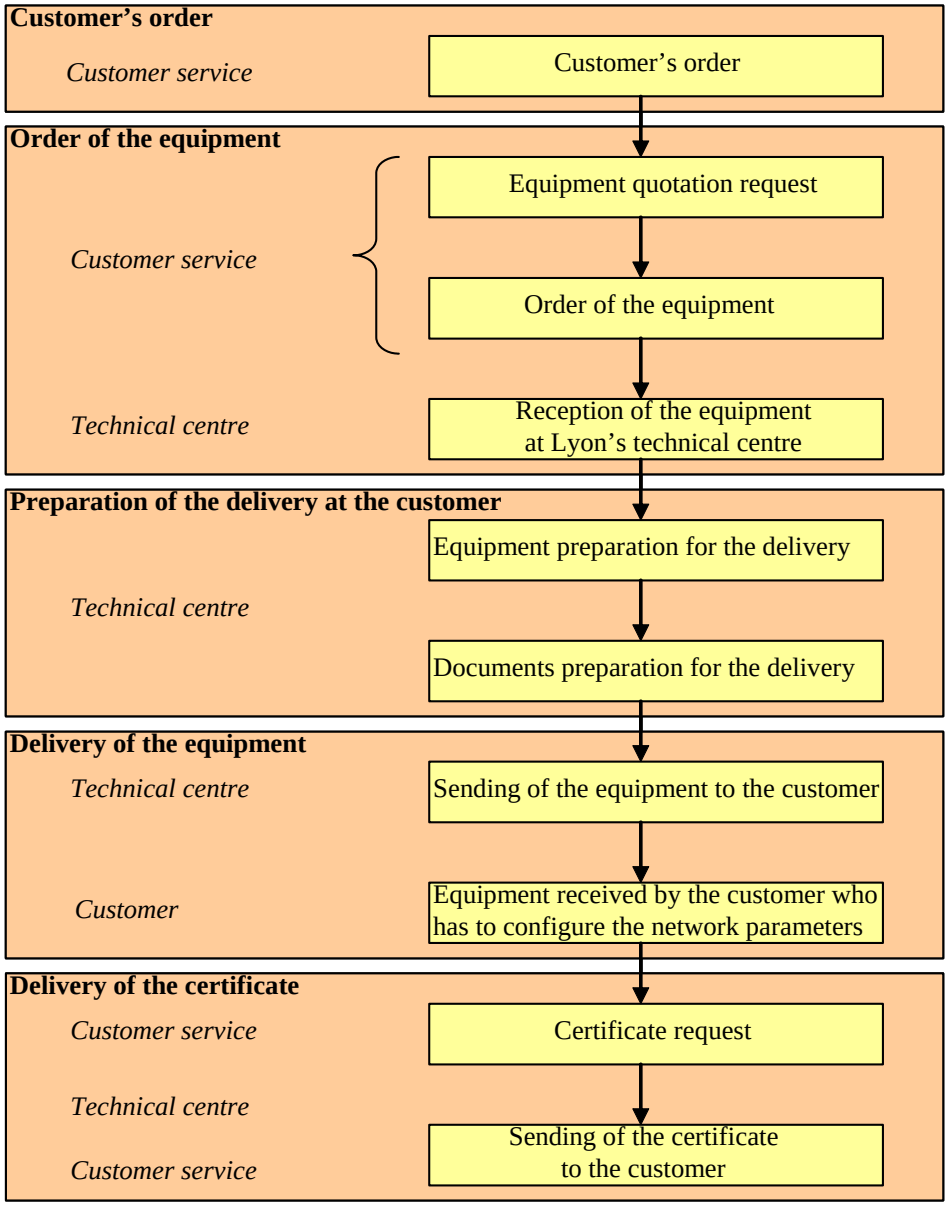

Figure 3 - Delivery process

In the evaluation context, the evaluator has considered as “product administrators” the “administrators” who visualize/acknowledge the alerts, activate/configure the agents and configure the correlation rules, and the “superusers” who have the same privileges that the “administrators” but can also create/configure users/administrators accounts. The evaluator has also considered as “product users” the “viewers” who visualize the alerts and the “analysts” who visualize/ acknowledge the alerts and can also activate/deactivate an agent (but they cannot configure it).

1.2.5. Evaluated configuration

The **SMP server** comes in the form of an *appliance* composed of the Red Hat Enterprise Linux 3.0 operating system, as well as the following applications:

- application SMP 2.7.3.5;
- server Tomcat 5.5.17;
- data-base MySQL 5.0.38;
- Java SDK 1.5.0-08;
- application GnuPG 1.2.1-20.

A **SMA agent** is composed of the following elements:

- application SMA 2.7.3.5 (identical Java application, whatever the system is);
- Java runtime JRE 1.5.0-06 (executable file dependent on the system on which the agent is installed).

The **SMA agents** are supported by the following operating systems:

- Linux : RedHat 7.1 or superior, RedHat Enterprise Linux 3.0 or superior, Debian 3.0 (kernel 2.4) or superior;
- Windows XP, 2000, 2003 ;
- SUN-Solaris 2.8 or superior;
- DEC TRU64 4.0f or superior;
- IBM-AIX 5.1 or superior.

The **SMC console** is accessible from a web browser like Mozilla Firefox 1.5 or superior or Internet Explorer 6.0. The evaluator has realized his tests from a Mozilla Firefox 2.0.0.5 web browser.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC], with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The evaluation technical report [ETR], delivered to DCSSI the 30th September 2008, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**passed**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has been analyzed by DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY]. They reveal the DSA algorithm used for the signature of archived data does not achieve the standard level. In order to remedy this, a recommendation is in the guides [GUIDES] indicating to escrow the signature public key of the archiving in a secure way.
All of the other results of the cryptographic analysis report [ANA-CRY] have been taken into account in the evaluator analysis of independent vulnerabilities. They did not highlight any exploitable vulnerability for the aimed VLA level.

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 “ExaProtect Security Management Solution (SMS), Version 2.7.3.5” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 2 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 summarized operational environmental security objectives specified in the security target [ST] and shall respect the recommendations in the guides [GUIDES], in particular:

1. OE.PROTECT_HARDWARE. The SMC console access work station and the SMP server shall be installed in secure premises.

2. OE.EXPORT_BASE. As part of the raw logs archiving service, it is supposed that the ways which enable the deciphering and the checking of the archives signature out of the TOE are managed in a secure way.

3. OE.TRUE_AGENT. The TOE shall rely on agents which transform in a reliable and consistent way the log entries related back by the equipment units.

4. OE.ADM_NO_EVIL. The organization shall recruit trustworthy staff as administrators for operating systems hosting the SMA ExaProtect agents and as administrators for the SMP ExaProtect server.

5. OE.HOST_CLEAN. The equipment on which the SMA agents are installed shall be made secure according to stiffening processes and updated according to specific vulnerabilities discovered on the operating system and the applications installed on these equipment units.

6. OE.SERVER_CLEAN. The appliance on which the SMP server is installed shall not contain other services (third applications) that the ones which are initially installed.

7. OE.USR_AWARE. The TOE users shall be trained to the use of the TOE and be sensitized to security, in particular to the consequences of their acts when they handle and acknowledge alerts.

8. OE.CRYPTO. The TOE shall use cryptographic mechanisms complying with the DCSSI referential for qualified products at the « standard » level.

9. OE.QUALIF. The TOE shall be evaluated at the EAL2+ level corresponding to a qualification at the standard level.

10. OE.TIME. The TOE time reference shall be synchronized with a time basis available by the environment.

11. OE.FIREWALL. The TOE environment shall include a communication filtering device located in front of the ExaProtect SMP server.

12. OE.CTL_AGENT_ASSETS. The systems on which the agents are installed shall implement an access control on agents' resources (configuration files, bi-key).

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 agreement[1], 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 countries[2], 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, 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 2+	Name of the component
ACM Configuration management	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**2**	Configuration items
	ACM_SCP			**1**	**2**	**3**	3	3		
ADO Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guidance	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Life-cycle support	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Evidence coverage
	ATE_DPT			**1**	1	**2**	2	**3**		
	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 Vulnerability assessment	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Guidance examination
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

*applied to FCS functional requirements.

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: Cible de sécurité ExaProtect Security Management Solution Reference SMSSecurityTarget.fr, version 1.8, 15/07/2008 ExaProtect
[ETR]	Evaluation technical report – Projet JOUBARBE Reference: OPPIDA/CESTI/JOUBARBE/RTE/1.0, 30/09/2008 OPPIDA
[ANA-CRY]	Cotation des mécanismes cryptographiques – Projet JOUBARBE, N°1228/SGDN/DCSSI/SDS/Crypto, 26/05/2008 SGDN/DCSSI
[CONF]	Liste de configuration de la version 2.7.3 Reference: ConfigListSMS273-fr, version 1.3, 22/09/2008 ExaProtect
[GUIDES]	Installation guidance: - SMA Installation Guide Reference : udoc-00616-en, version 6, 23/04/2008 ExaProtect - SMP Installation Guide Reference : udoc-00614-en, version 7, 23/04/2008 ExaProtect Administration guidance: - SMS Administration Guide Reference : udoc-00632-en, version 3, 23/04/2008 ExaProtect User guidance: - SMA User Guide Reference : udoc-00613-en, version 6, 22/04/2008 ExaProtect

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for 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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[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.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR