PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-2009/20

ID One™ ePass v2.1 with configuration BAC on NXP P5CD040V0B, P5CD080V0B, P5CD144V0B

Paris, 23rd 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 ANSSI (French Network and Information Security Agency), 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
Agence nationale 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

ANSSI-2009/20

Product name

ID One™ ePass v2.1 with configuration BAC on NXP P5CD040V0B, P5CD080V0B, P5CD144V0B

Product reference

Revision 1 with optional code (patch) r2.

Protection profile conformity

[PP BAC] BSI-PP-0017

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 4 augmented

ALC_DVS.2

Developers

Oberthur Technologies[1]
50 quai Michelet
92300 Levallois-Perret, France

NXP Semiconductors GmbH[1]
Stresemannallee 101
D-22502 Hamburg, Germany

Sponsor

Oberthur Technologies
50 quai Michelet, 92300 Levallois-Perret, France

Evaluation facility

CEACI (Thales Security Systems – CNES)
18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France
Phone: +33 (0)5 61 28 16 51, email : nathalie.feyt@thalesgroup.com

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

1: these are the main sites.

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 French Network and Information Security Agency 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 sponsors 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 the smart card “ID One™ ePASS v2.1 with configuration BAC embedded on NXP P5CD040V0B, P5CD080V0B, P5CD144V0B revision 1 with the optional code (patch) r2” developed by Oberthur Technologies and NXP Semiconductors.

The evaluated product is a contactless smartcard with its antenna. It implements the travel document features according to the specifications from the International Civil Aviation Organization (cf. [ICAO]). The contactless microcontroller with embedded software allows to check the authenticity of the travel document, and to identify its holder during a border control, with the support of an inspection system. In particular, it enables:

- Protection in integrity of the holder’s data stored by physical means and thanks to the access control which allows only one writing;
- Authentication between the travel document holder and the inspection system prior to any border control by the Basic Access Control (BAC);
- Protection in integrity and confidentiality of data read by the secure messaging;
- Authentication of the genuine chip by the Active Authentication mechanism (if activated);

The chip and its embedded software are intended to be inserted into the cover page of traditional passport booklets. They can be integrated into modules or inlay. The final product can be a passport, a plastic card, etc.

1.2. Evaluated product description

The security target [ST], in chapter 2, defines the evaluated product, its evaluated security functionalities and its operation environment.

The security target conforms to the protection profile [PP BAC]. The evaluator considers the conformity as demonstrable. Indeed, the security target as been written following the version 3.1 of [CC] whereas the protection profile [BAC] has been certified according to the version 2.3 of [CC].

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:

Command Vs. Chip	**P5CD0040**	**P5CD0080**	**P5CD0144**
ATS (Answer To Select)	4F 54 49 44 **25** 94 XX XX XX XX	4F 54 49 44 **28** 94 XX XX XX XX	4F 54 49 44 **2B** 94 XX XX XX XX

In addition, reading the file EF.TOE by the command Read Binary allows getting the following identifications information:

Identification Information	**Value examples**
Code ROM ID	04 03 06 95 91
Patch ID	04 03 07 09 42
[PP EAC] ID	04 01 26
[PP BAC] ID	04 01 17
Support of EAC/AA /BAC security features	04 01 0X, where X = b1|0|b2|b3 with: b1 = EAC, here = 0 b2 = AA b3 = BAC, here = 1

1.2.2. Security services

The product provides mainly the following security services:

- Access control in reading;
- Access control in writing;
- BAC mechanism;
- Secure messaging mechanism;
- Personalization agent authentication;
- Active Authentication mechanism with RSA and ECC;
- Self tests;
- Safe state management;
- Physical protection.

The microcontroller provides the following security services:

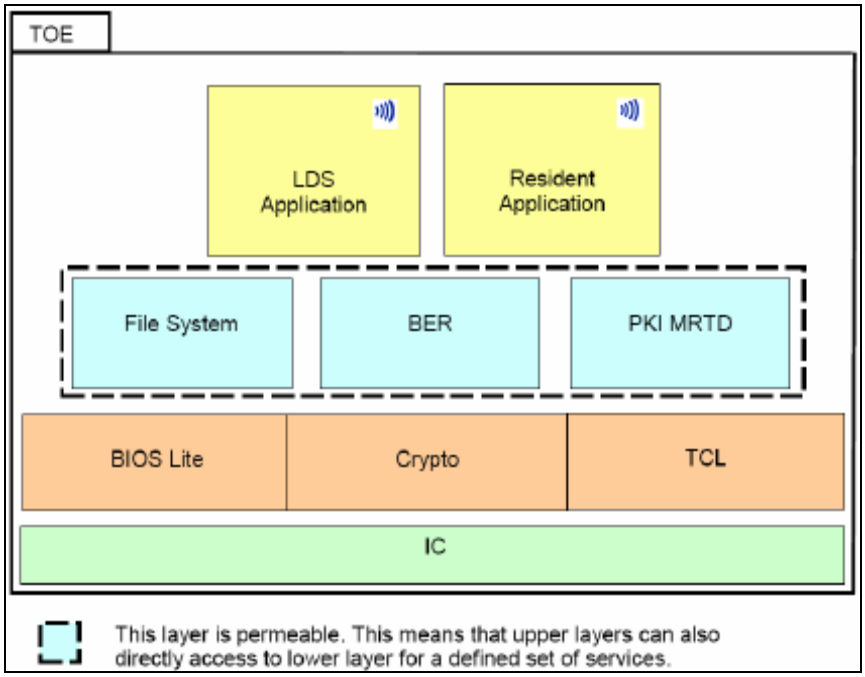
- Random number generator;
- Triple DES coprocessor;
- Control of operating conditions;
- Protection against physical manipulations;
- Logical protection;
- Protection of control mode;
- Memory access control;
- Special Function Register access control.

1.2.3. Architecture

The product consists of:

- A layer corresponding to the hardware (IC) ;
- A low level layer providing an interface between the hardware and the upper layer :
  - BIOS Lite manages memory access (read, write) and other basic manipulation of the hardware;
  - Crypto provides cryptographic services;
  - TCL handles the communication interface (i.e. contactless interface);
- A layer providing generic APIs:
  - File System manages data application in a secure way;
  - BER provides a toolbox to manage APDU format;
  - PKI MRTD provides generic functions for Activation Authentication and Secure Messaging of incoming and outgoing commands;
- An application layer:
  - LDS Application implements the commands of e-passport that are available in operational phase;
  - Resident Application Implements the commands of e-passport that are available in pre-personalization and personalization phases.

The following figure summarizes this architecture:



1.2.4. Life cycle

The product's life cycle is organised as follow:

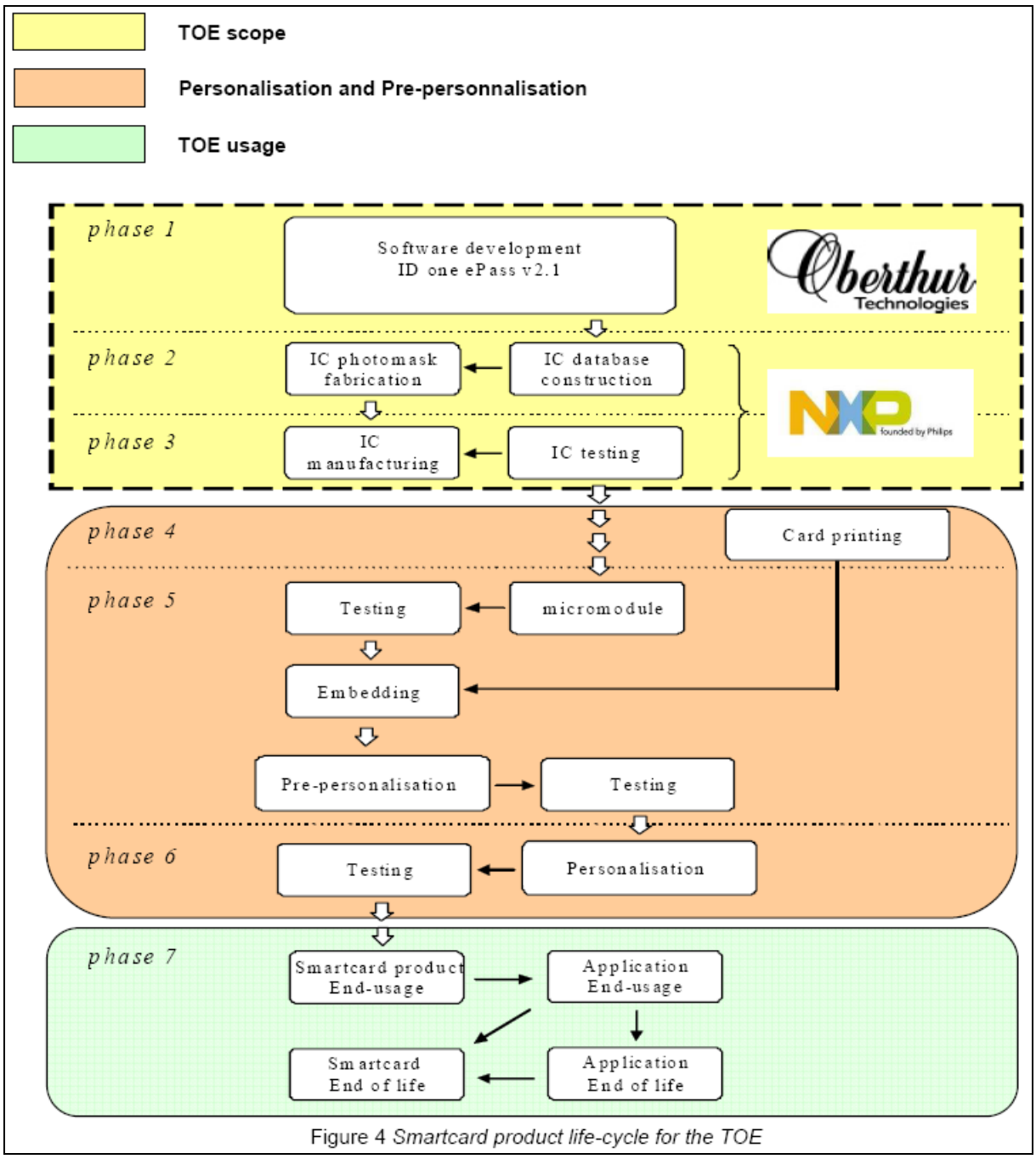


Figure 4 *Smartcard product life-cycle for the TOE*

Product delivery from chip manufacturer to pre-personalizer is protected by specific security measures.

Loading of functional patches and pre-personalization is out of the evaluation scope. These steps are covered by guides and specific security measures.

The product has been developed by Oberthur Technologies on the following sites:

Oberthur Technologies - Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies - Levallois

50, quai Michelet
92 300 Levallois-Perret
France

Oberthur Technologies - Bordeaux

Parc Scientifique UNITEC 1
4, allée du Doyen Georges Brus - Porte 2
33 600 PESSAC
France

The microcontrollers have been developed and manufactured by NXP on the sites specified in [BSI-DSZ-CC-0404-2007] / [BSI-DSZ-CC-0410-2007] / [BSI-DSZ-CC-0411-2007]. The main one is:

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Germany

In the evaluation context, the evaluator has considered:
- Product administrator, the nations issuing the passport;
- Product user, passport holders and inspection systems which are involved in the use phase of the product.

1.2.5. Evaluated configuration

The product can be personalized with different configurations.

The certificate applies to the following configurations:
- BAC mechanism activated;
- EAC mechanism deactivated;
- Active Authentication mechanism activated (ECC or RSA) or deactivated;
- Contact interface deactivated;
- Get Data command deactivated.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC], with the Common Evaluation Methodology [CEM].
For assurance components not covered by the [CEM], the evaluation facility own evaluation methods, validated by ANSSI, have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

2.2. Evaluation work

The evaluation has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness comes from the integration of the software in the microcontroller already certified.

Therefore, the results of the evaluation of the microcontroller P5CD040V0B, P5CD080V0B, P5CD144V0B at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile, have been used. This microcontroller has been certified by the BSI the (cf. [BSI-DSZ-CC-0404-2007] / [BSI-DSZ-CC-0410-2007] / [BSI-DSZ-CC-0411-2007]).

The evaluation technical report [ETR], delivered to ANSSI on 12th may 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 been analysed by ANSSI. The results are stated in the cryptographic analysis report [ANA-CRY] and have been taken into account in the evaluator vulnerability analysis.

The analysed mechanisms contain, for some of them, implementations that are not conformant to ANSSI cryptographic referential (Cf. [REF-CRY]).

2.4. Random number generator analysis

The hardware random number generator has been evaluated by the German evaluation facility T-Systems with the [AIS 31] methodology (cf. [BSI-DSZ-CC-0404-2007] / [BSI-DSZ-CC-0410-2007] / [BSI-DSZ-CC-0411-2007]).

The hardware generator reaches the class "P2-High" according to [AIS 31].

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of 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 ID One™ ePass v2.1 with configuration BAC on NXPP5CD040V0B, P5CD080V0B, P5CD144V0B, revision 1.0 with optional code (patch) r2.0 developed by Oberthur Technologies, submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 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] paragraphs 7.4, 7.5, 9.3, 9.4 and 9.5.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released 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:

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

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[1], 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 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 4+	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**	**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 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 procedure
ALC Life-cycle support	ALC_CMC		**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
	ADO_DEL		**1**	1	**1**	1	1	**1**	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	**1**	**1**	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well defined development tools
ST Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	2	**3**	3	**4**	**2**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant testing, sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**3**	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation : - HEIMDALL – Security Target – BAC reference FQR: 110 4292, revision 3 Oberthur Technologies For the needs of publication, the following security target has been provided and validated in the evaluation : - ID One™ ePass v2.1 with BAC configuration Public Security Target FQR 110 4641, revision 1 Oberthur Technologies
[RTE]	Evaluation Technical Report - Project: HEIMDALL Reference HEI_ETR, revision 1.0 Thales Security Systems – CEACI business activity
[ANA-CRY]	Cryptographic analysis report of the DCSSI : - Cotation de mécanismes cryptographiques Qualification HEIMDALL N°1469SGDN/DCSSI/DR du 9 juin 2009 SGDN/DCSSI
[CONF]	HEIMDALL – configuration List FQR: 110 4535, revision 1 Oberthur Technologies
[GUIDES]	HEIMDALL - Administration and User Guidance Document FQR 110 4404, revision 5 Oberthur Technologies
[PP BAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0017*
[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2, 19 November 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0026*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.*
[ICAO]	ICAO Doc 9303, Sixth Edition, 2007

[BSI-DSZ-CC-0404-2007]	NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-DSZ-CC-0404-2007*
[BSI-DSZ-CC-0410-2007]	NXP Secure Smart Card Controller P5CD080V0B, P5CN080VOB and P5CC080VOB each with specific IC Dedicated Software *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-DSZ-CC-0410-2007*
[BSI-DSZ-CC-0411-2007]	NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-DSZ-CC-0411-2007*

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, 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 IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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, current version, see www.ssi.gouv.fr
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)