Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-2012/43

Athena IDProtect/OS755 Key version 9.1.2
on AT90SC25672RCT-USB Microcontroller embedding IDSign applet

Paris, August 10th 2012

Courtesy Translation

SÉCURITÉ CERTIFICATION

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 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
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2012/43

Product name

Athena IDProtect/OS755 Key version 9.1.2 on AT90SC25672RCT-USB Microcontroller embedding IDSign applet

Product reference

- **Athena IDProtect/OS755 Java Card : release date 0113, release level 2109**
- **Inside Secure AT90SC25672RCT-USB : AT58829, revision D**
- **Inside Secure Toolbox : version 00.03.11.05**
- **Athena IDSign : version 3.0, build 001, AID class** A0 00 00 01 64 49 44 53 69 67 6E 01

Protection profile conformity

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04

[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Evaluation criteria and version

Common Criteria version 3.1 revision 3

Evaluation level

EAL 4 augmented

AVA_VAN.5

Developer(s)

Athena Smartcard Inc.
20380 Town Center Lane – Suite 240
Cupertino CA95014,
United States of America

Inside Secure S.A.
Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR,
Scotland, United Kingdom

Sponsor

Athena Smartcard Solutions
1-14-16, Motoyokoyama-cho, Hachioji-shi
Tokyo, 192-0063, Japan

Evaluation facility

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, modified. 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.

Contents

1. The product

1.1. Presentation of the product

The evaluated product is « Athena IDProtect/OS755 Key version 9.1.2 on INSIDE Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet ». The product is developed by Athena Smartcard Solutions and embedded on the AT90SC25672RCT-USB microcontroller developed by Inside Secure. It can be in the form of a Smartcard or a USB token. This product is designed to be used as part of applications providing Digital Signature capabilities.

1.2. Evaluated product description

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

The security target is based on the protection profiles certified under references [BSI-PP-0005-2002] and [BSI-PP-0006-2002], with necessary adjustments to match Common Criteria version 3.1 [CC] (these PP were certified according to version 2.1).

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, that are returned by the product as a response to the GET DATA command using the tag 9F7F (refer to [GUIDES], section 2.5 and 2.6 of the Preparative Guide and section 1.1 of the Operational Guide) :

Data Element	Length	Chip Serial Number or default
IC fabricator	2	'4180'
IC type	2	'0106'
Operating system identifier	2	'8211'
Operating system release date	2	'0113'
Operating system release level	2	'2109'
IC fabrication date	2	IC production date (SII_2 & SII_3)
IC serial number	4	Die number ('00'+ SII_6 + SII_7 + SII_8)
IC batch identifier	2	Lot number (SII_4 & SII_5)
IC module fabricator	2	'0000'
IC module packaging date	2	'0000'
ICC manufacturer	2	'0000'
IC embedding date	2	'0000'
IC pre-personalizer	2	'0000000000000000'
IC pre-personalization date	2	
IC pre-personalization equipment identifier	4	
IC personalizer	2	'0000000000000000'
IC personalization date	2	
IC personalization equipment identifier	4	

In order to illustrate this operation, below is the result of a validation performed by the evaluator on a sample of the product:

- Command GET DATA with tag **9F7F** sent :
  - 00CA**9F7F**00 ;
- Data returned by the product :
  - 4180 0106 8211 **0113 2109** 0954 00231909 6598 0000 0000 0000 0000 0000000000000000 0000000000000000

In the returned data, we can identify, in particular, the values **0113** and **2109** (corresponding to the fields " *Operating System release date* " and " *Operating System release level* " in the table above). These elements correspond to the whole embedded software including the OS IDProtect and the applet IDSign.

In addition, the command GET DATA with tag **0046** can be used to retrieve the elements that identify the component. On the evaluated sample, we obtain :

- Command GET DATA with tag **0046** sent :
  - 00CA**0046**00 ;

- Data returned by the product :
    - **2303**09546598231909

The value **23** identifies the component. It corresponds to the value in IC register SN_0 (here the AT90SC25672RCT-USB). Furthermore, the value **03** provides the revision of the component corresponding to the IC register SN_1 (here revision D).

1.2.2. Security services

The product provides mainly the following security services:

- signature creation : the product signs the data to be signed (DTBS – *Data To Be Signed*) using the signature private key (SCD – *Signature Creation Data*) ;
- identification and authentication : the product handles the identification and authentication of the signatory and the administrator; it also enforces a mechanism of role separation ;
- access control : the product verifies that for each operation initiated by a user, the security attributes, corresponding to the privileges granted for a user to access the data, are valid ; typical operations of the SSCD, such as the digital signature, the key generation, the import and export of SCD/SVD (*Signature Creation Data / Signature Verification Data*, which are the private/public keys for signature) and the verification of the RAD/PUK (*Reference Authentication Data / PIN Unblocking Key*, which are the PIN code and the unlock code of the product), are subject to these verifications ;
- secure channel : the product can set up a communication channel that is secured between itself and the external device that it interacts with ; typical operations of the SSCD, such as the digital signature, the key generation, the import and export of SCD/SVD and the verification of the RAD/PUK, are subject to the establishment of this secure channel ;
- cryptography : the product offers cryptographic means to all other security functions (in particular, DES/TDES, RSA, RNG, prime number generation) ;
- protection: the product protects the data of the security functions (“*TSF data”*), the data of the user (“*user data”*) and the security functions (“*TSF”*) against malfunction, perturbation and observation using autotests, the management of crashes, the integrity tests, the secure re-initialization, the counter-measures to prevent leakage, etc. The security service also ensures the termination of the card content loading and installation services, the patch loading process and its termination.

1.2.3. Architecture

The final product can be in the form of a smartcard, or a USB token, as the underlying component AT90CS25672RCT-USB provides both the ISO7816 and USB interfaces.

The TOE does not provide any other external interface.

All application software is embedded in ROM and only patches are loaded in EEPROM.

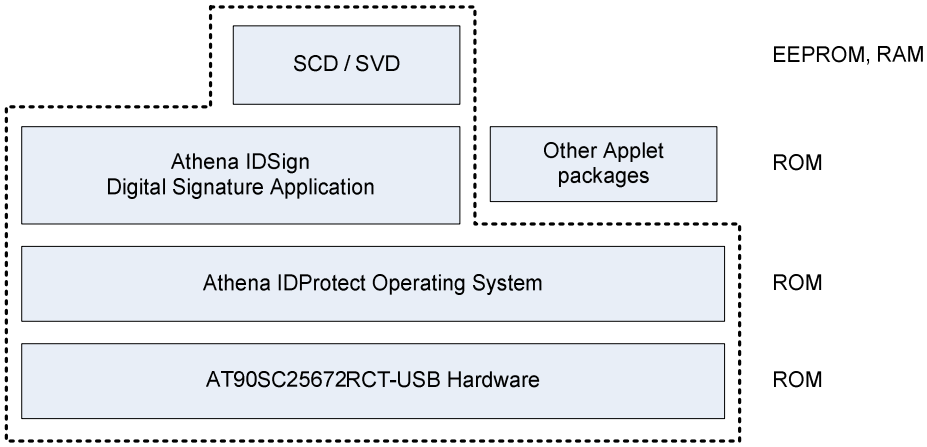
The TOE (*Target Of Evaluation*) includes:

- the component :
    - INSIDE Secure AT90SC25672RCT-USB : AT58829, revision: D, developed by Inside Secure S.A. ;
- associated with the crypto library :

  - INSIDE Secure Toolbox, version: 00.03.11.05, developed by Inside Secure S.A. ;
- embedding the Operating System :
  - Athena IDProtect 9.1.2, release Date '0113', release Level '2109', ROM code release Level '0109', EEPROM code Patch Level '2xxx' includes patches: PID01 to PID07, developed by Athena Smartcard ;
- and the application :
  - Athena IDSign, Applet class AID = A0 00 00 01 64 49 44 53 69 67 6E 01, version 3, Build 001, developed by Athena Smartcard.

The other applet packages are not instantiated and are deleted before the personalisation phase.

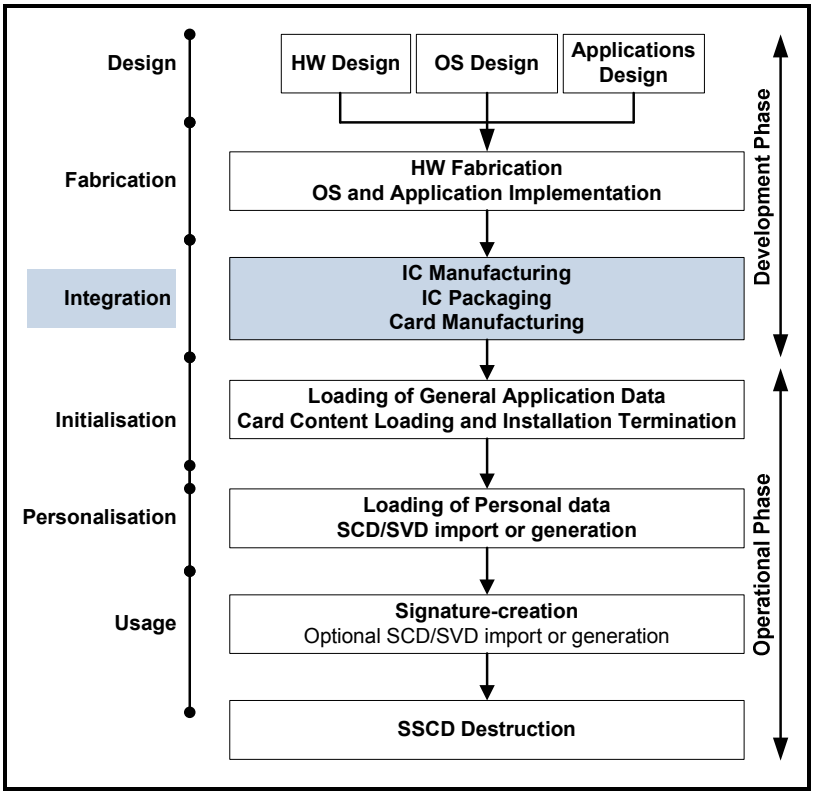
The perimeter of the TOE is illustrated in the following picture (boundaries in dotted-line):



TOE Physical Boundaries

1.2.4. Life cycle

The product's life cycle is based on the smartcard lifecycle, as described in the protection profiles [BSI-PP-0005-2002] and [BSI-PP-0006-2002], but refined with the addition of a step called "*Integration*". It is illustrated in the following picture:



The delivery point is located at the end of step "*Integration*", stating the end of the product development phase.

All the steps that precede this delivery point have been covered by this evaluation (as part of ALC), if necessary by reusing results obtained during the evaluation of the underlying component.

The product has been developed on the following sites:

- Software development sites :
  - **Athena Smartcard Ltd.**
    Westpoint - 4 Redheughs Rigg - South Gyle
    Edinburgh EH12 9DQ
    Scotland - United Kingdom
  - **Athena Smartcard Inc.**
    20380 Town Center Lane – Suite 240
    Cupertino CA95014
    United States of America
- Hardware development and IC manufacturing site :
  - **Inside Secure S.A.**
    Maxwell Building
    Scottish Enterprise technology Park,
    East Kilbride, G75 0QR
    Scotland - United Kingdom

In the evaluation context, the role “administrator” (“S.Admin”) has been considered as the product administrator and the role “signatory” (“S.Signatory”) has been considered as the product user (see [ST] section 4.2 Subjects).

1.2.5. Evaluated configuration

The certificate applies to the configuration of the TOE obtained after following the preparative guide (see [GUIDES]). This guide describes the options of personalization that have to be chosen in order to obtain the evaluated TOE configuration. Additional personalization options are possible but do not correspond to the evaluated configuration.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 3** [CC], with the Common Evaluation Methodology [CEM].

For assurance components which are not covered by [CEM] manual, 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. Thus the reached AVA_VAN level has been determined according to the rating table of the [CC AP] guides that is more demanding than the default one defined in [CC] used for other types of products (software products for example).

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 "AT90SC25672RCT-USB D rev. D" at EAL4 level augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the ANSSI protection profile (see [PPCR98_06]), have been used. This microcontroller has been certified by the ANSSI under the reference [DCSSI-CC-2006_30] on December 19th 2006.

The microcontroller robustness level has been confirmed on January 16th 2012 (see [SUR_IC]) in a surveillance process.

The evaluation has also taken into account the result of the surveillance of the cryptographic library "Cryptographic library ATMEL toolbox 00.03.11.05" which was initially certified at level EAL5 augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 (see [ANSSI-CC-2009_11] and [SUR_Biblio]).

Finally, the evaluation has also taken into account the result of the two previous versions of the product. Two ANSSI certificates were issued then (see [ANSSI-CC-2011_03] and [ANSSI-CC-2011_45]).

The evaluation technical report [ETR], delivered to ANSSI the 23th of July 2012, 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 against the ANSSI technical referential [REF-CRY]. Nevertheless, the evaluation has not lead to the identification of any exploitable vulnerability for the targeted AVA_VAN.5 level.

2.4. Random number generator analysis

The analysis of the random number generator against the ANSSI technicals referentials was out of the scope of this evaluation and was not performed.

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 “Athena IDProtect Key (Smartcard or USB token) version 9.1.2 - Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet” 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 security objectives for the operational environment, as specified in the security target [ST], and shall respect the recommendations in the guidance [GUIDES].

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 2010 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High 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, 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 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 procedures
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
	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									
	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 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**	1	**3**	3	**4**	**1**	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**	Independent testing: sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - Athena IDProtect Key – Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB embedding IDSign applet Security Target, version 1.1, 02/12/2011, Athena Smartcard. For the needs of publication, the following security target has been provided and validated in the evaluation: - Athena IDProtect Key – Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB embedding IDSign applet - Security Target Lite, version 1.1, 02/12/2011, Athena Smartcard.
[ETR]	Evaluation technical report : - Evaluation technical report - Project: BOREALIS_M02, version: 2.0, 23/07/2012, Thales-CEACI.
[CONF]	Product configuration List : - Borealis_M02 - Documents Configuration List – Borealis Project, version 2.0, 02/12/2011 Athena Smartcard.
[GUIDES]	Preparation guidance: - Preparative Procedures, Athena IDProtect Key version 1.0, 02/12/2011, Athena Smartcard. - Athena IDProtect Key, Card Administrator Manual, version 1.0, 02/12/2011, Athena Smartcard. - Athena IDProtect Transport Key Application Note version 0.2, 29/06/2010 Athena Smartcard. User guidance: - Operational User Guidance, Athena IDProtect Key version 1.0, 02/12/2011, Athena Smartcard.

[BSI-PP-0005-2002]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certified by the BSI under the reference BSI-PP-0005-2002T.*
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certified by the BSI under the reference BSI-PP-0006-2002T.*
[PPCR98_06]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certified by the ANSSI under the reference PP/9806.*
[DCSSI-CC-2006_30]	ANSSI Certificate delivered on December 19th 2006 for the product: « Microcontrôleur sécurisé ATMEL AT90SC25672RCT-USB rev. D ».
[SUR_IC]	Surveillance letter emitted by the ANSSI on January 16th 2012 for the product: « Microcontroleur sécurisé ATMEL AT90SC25672RCT-USB, rev. D » initially certified by the ANSSI (see [ANSSI-CC-2006_30]).
[ANSSI-CC-2009_11]	ANSSI certificate delivered on June 30th 2009 for the evaluation of the library: « Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 ».
[SUR_Biblio]	Surveillance letter emitted by the ANSSI on March 18th 2011 for the library: « Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 » initially certified by the ANSSI (see [ANSSI-CC-2009_11]).
[ANSSI-CC-2011_03]	ANSSI certificate delivered on March 4th 2011 for the product: « SafeNet eToken (Smartcard or USB token) Version 9.1 - Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller embedding IDSign applet ».
[ANSSI-CC-2011_45]	ANSSI certificate delivered on September 22nd 2011 for the product: « SafeNet eToken (Smartcard or USB token) Version 9.1.2 - Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet ».

Annex 3. Certification references

Decree number 2002-535, 18th April 2002, modified 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, 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 IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 dated 26 January 2010 attached to the Référentiel général de sécurité, see www.ssi.gouv.fr.