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-2010/57

CC IDeal Citiz SmartCard (on SB23YR48B), version 1.4.5 IAS ECC application with PIN or MOC authentication

Paris, 17th September 2010

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 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-2010/57

Product name

CC IDeal Citiz SmartCard (on SB23YR48B)- IAS ECC application with PIN or MOC authentication

Product reference, version

IDEALMOC/SB23YR48/1.4.5, Version 1.4.5

Protection profile conformity

[PP0005], Secure Signature-Creation Device Type 2, version 1.04

[PP0006], Secure Signature-Creation Device Type 3, version 1.05

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 5 augmented

ALC_DVS.2, AVA_VAN.5

Developers

SAGEM Sécurité

Etablissement d'Osny, 18 Chaussée Jules César, 95520 Osny, France

ST Microelectronics

29 Boulevard Romain Rolland, 75669 Paris cedex 14, France

Sponsor

SAGEM Sécurité

Etablissement d'Osny, 18 Chaussée Jules César, 95520 Osny, France

Evaluation facility

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Phone: +33 (0)4 38 78 40 87, email : cesti.leti@cea.fr

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 the « CC IDeal Citiz smartcard (on SB23YR48B), IDEALMOC/SB23YR48/1.4.5, Version 1.4.5 » developed by SAGEM Sécurité and ST Microelectronics.

The evaluated product is a dual smartcard (contact and contactless). It is composed of:

- three applications :
  - the AIP application which performs the pre-personalization and the personalization operations of the smartcard. This application is not accessible once in Operational Use phase,
  - the ICAO application which implements the machine readable travel document features and which may be instantiated several times on the product,
  - the IAS (Identity Authentication Signature) application which allows to generate, destroy and load keys to generate digital signature.
- and an opened JacaCard System which allows to load applets on the product during its Operational Use phase.

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 conformant to the[PP0005] and [PP0006] protection profiles, adapted to the CC version 3.1 (as those PP has been written according to the CC 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:

- product's name and version : CC Ideal Citiz, version 1.4.5;
- microcontroller's name and version: SB23YR48B;
- commercial reference (SAGEM) : IDEALMOC/SB23YR48/1.4.5;
- whole embededd software reference (SAGEM ORGA) OFFICIEL_IDEAL_ST23YR80_1_4_50;
- ST Microelectronics reference: SB23YR48 QPX (masked chip).

Every version of the software components of the certified version of the product can be checked according to the command and responses identified in the installation guidance of the product (see [GUIDES]).

1.2.2. Security services

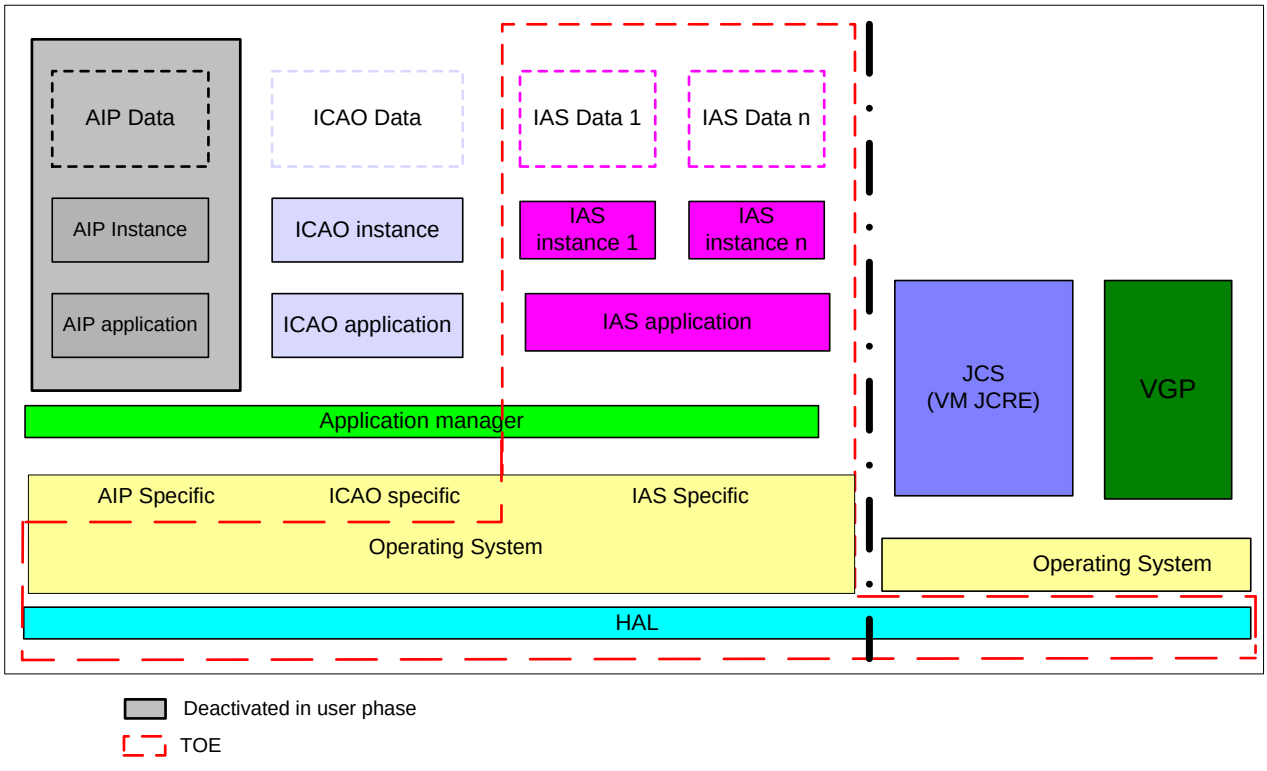
The TOE provides mainly the following evaluated security services:

- generation of private and public signing keys ;
- destruction of the private and public signing keys ;
- import of private signing key;
- signature creation (based on RSA or elliptic curves mechanisms);
- PIN or biometric fingerprint (Match On Card method) authentication of the signatory.

1.2.3. Architecture

The product consists of

- the SB23YR48B microcontroller, developed and produced by ST Microelectronics ;
- software parts, developed by SAGEM Sécurité, which CVS reference is OFFICIEL_IDEAL_ST23YR80_1_4_00, masked in the microcontroller's ROM, composed of:
  - the OPUCE operating system;
  - the HAL hardware abtract layer;
  - the JacaCard System;
  - the AIP card initialization and personalization application;
  - and the IAS and ICAO applications ;
- the IAS application patch, version 5.0, developed by SAGEM Sécurité, loaded into the microcontroller's EEPROM.

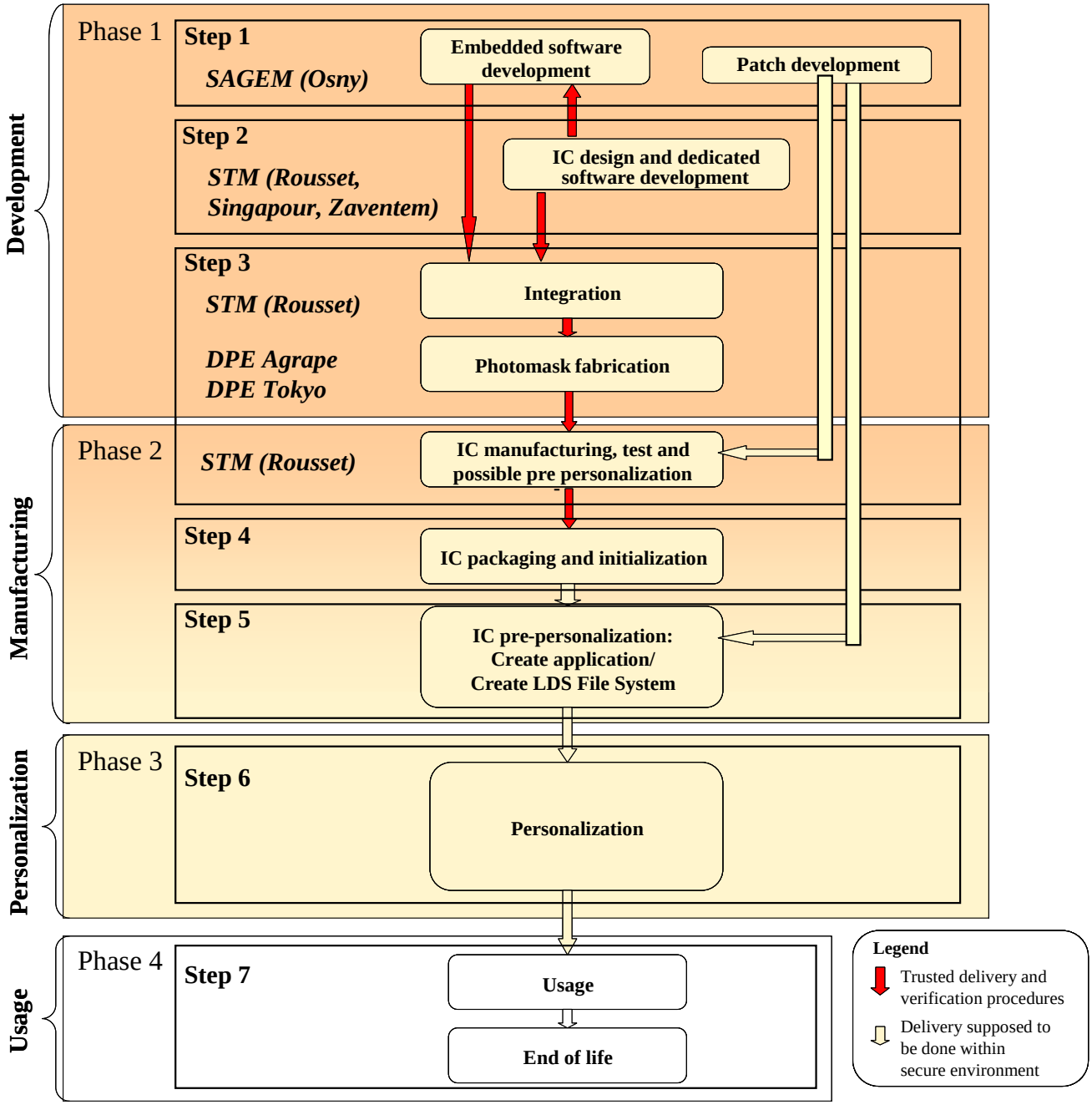


The TOE is the IAS Application, together with the functions/services provided by the operating system and the microcontroller IC required to support the applet functionalities.

The evaluation facility verified the isolation between the various applications, notably between those in the TOE with those not included in the TOE. The evaluation facility verified that a Java applet could only access to its own data and not to those belonging to another applet.

1.2.4. Life cycle

The product's life cycle is organised as follow:



Patch loading is protected by the AIP application.

The embedded software has been developed on the following site:

SAGEM Sécurité - Etablissement d'Osny

18 Chaussée Jules César
95520 Osny
France

The microcontroller development sites are identified in the [2010/02] certification report.

1.2.5. Evaluated configuration

The certificate applies to the opened configuration of this product (applets can be loaded on the product in operational phase, phase 7).
The product tested by the evaluation facility is typical to the final product.

The signatory's authentication method, PIN or MOC, is decided in the personalization phase of the smartcard. Administration guidance of this product provides description of the objects that need to be created to use one of those two authentication methods. User guidance describes the services allowing to use those objects as well as the security measures that have to be applied to meet the [ST] security objectives.

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]

In order to meet the specificities of smart cards, the [CC AP] and [COMP] 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 "SB23YR48B with Neslib version 3.0" at EAL6 level augmented with ALC_FLR.1, compliant with the [PP0035] protection profile, have been used. This microcontroller has been certified the 10 February 2010 under the reference ANSSI-CC-2010/02. The maintenance report ANSSI-2010/02-M01 has also been issued the 19th March 2010 for this product.

The evaluation relies on the evaluation results of the « CC IDeal Citiz SmartCard (on SB23YR48B), version 1.4.5 » product certified, according to [PP0005] and [PP0006], under the reference ANSSI-CC-2010/22.

The evaluation technical report [ETR], delivered to ANSSI the 10th September 2010, 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 according to [REF-CRY]. The results are stated in the cryptographic analysis report [ANA-CRY] which concludes that:

- the ECDSA signature schema offered by this product does not conform to the referential;
- signature must be generated using the SHA-224 or SHA-256 functions;
- RSA modules and elliptic curves must be sized according to the referential rules;
- for the RSA signature schema, it is recommended to use a public exponent higher than $2^{16.}$

Those results have been taken into account in the evaluator independent vulnerability analysis and had not leaded to the identification of exploitable vulnerability for the aimed AVA_VAN level.

2.4. Random number generator analysis

The random number generator used by this product is the one provided by the microcontroller (see [2010/02] certification report).

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 "CC IDeal Citiz SmartCard (on SB23YR48B), version 1.4.5" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 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 specified in the security target [ST] at the 4.2 and 4.3 chapters, and shall respect the recommendations in the guidance [GUIDES].

As the sensors are note included in the considered evaluation perimeter the evaluated product do not prevent against false fingerprint.

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 5+	Name of the component
ADV Developmentt	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semiformal 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	1	2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_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	2	Compliance with implementation standards
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	3	Testing: modular 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

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 5+	Name of the component
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Focused vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - « Common Criteria security target – IAS ECC – Secure Signature Creation Device – CC IDeal Citiz », reference SSE-0000078723, révision 01,, For the needs of publication, the following security target has been provided and validated in the evaluation: - « Common Criteria security target lite – IAS ECC – Secure Signature Creation Device – CC IDeal Citiz », reference SSE-0000078793, révision 02.
[ETR]	Evaluation technical report : - « Réévaluation EOS - Rapport Technique d'Evaluation », reference LETI.CESTI.EOS.RTE.002, édition 3.2, - « Réévaluation EOS (avec MOC) - Rapport Technique d'Evaluation », reference LETI.CESTI.EOS.RTE.003, édition 1.1.
[ANA-CRY]	« Cotation de mécanismes cryptographiques- Qualification EOS », n° 805/ANSSI/ACE/LCC du 2 avril 2010.
[CONF]	« IDEAL_– Software Release Sheet – V1.4.50», reference SSE-0000075528, révision 22.
[GUIDES]	Installation guidance: - «« IDEAL 1.4 procédure d'installation », reference SSE-0000076822, version 01, Administration guidance: - « IDEAL – IAS ECC Functionnal specification », reference SSE-0000067235, version 02, - « ICAO Application Pre-personalization manual - Project : CC Ideal Pass », reference SSE-0000074722, version 02, - « IDEAL IAS ECC Personalization Guidance », reference: SSE-0000064845, version 03, - « ICAO Application Personalization manual - Project : CC Ideal Pass », reference SSE-0000074723, version 04, User guidance: - « ICAO Application User manual - Project : CC Ideal Pass », reference SSE-0000074862, version 01, - « IDEAL IAS ECC Operational User Guidance », reference: SSE-0000065958, version 02.
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the referenc BSI-PP-0005-2002.*

[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0006-2002.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*
[2010/02]	Certification report ANSSI-CC-2010/02, issued the 10th February 2010 for the "SA23YR48/80B and SB23YR48/80B, secured microcontrollers including the cryptographic libray NesLib v2.0 or v3.0 in SA or SB configuration".
[2010/02-M01]	Maintenance report ANSSI-2010/02-M01, issued the 19th March 2010, related to the ANSSI-CC-2010/02 certificate.

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, 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 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, 8th January 2010, Management Committee.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.11, 24th of October 2008, see www.ssi.gouv.fr