



*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-2014/74**

### **SOMA-c003 – EAC, SAC and AA applications, version 1.3**

*Paris, 22<sup>nd</sup> October 2014*

**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](mailto:certification.anssi@ssi.gouv.fr)

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



<i>Certification report reference</i>	<b>ANSSI-CC-2014/74</b>	
<i>Product name</i>	<b>SOMA-c003 – EAC, SAC and AA applications</b>	
<i>Product reference</i>	<b>Version 1.3</b>	
<i>Protection profile conformity</i>	<p><b>BSI-CC-PP-0056-V2-2012-MA-02, [PP EAC], version 1.3.2 Machine Readable Travel Document with “ICAO Application”, Extended Access Control</b></p> <p><b>BSI-PP-0068-V2-2011, [PP PACE], version 1.0 Machine Readable Travel Document using Standard Inspection Procedure with PACE, Extended Access Control</b></p>	
<i>Evaluation criteria and version</i>	<b>CC version 3.1 revision 4</b>	
<i>Evaluation level</i>	<p><b>EAL 4 augmented</b></p> <p><b>ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5</b></p>	
<i>Developer(s)</i>	<p><b>Arjowiggins Security SAS –</b> <b>Gep S.p.A.</b> Viale Remo De Feo 1, 80022 Arzano (NA), Italy</p>	<p><b>STMicroelectronics</b> 190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 ROUSSET, France</p>
<i>Sponsor</i>	<p><b>Arjowiggins Security SAS – Gep S.p.A.</b> Viale Remo De Feo 1, 80022 Arzano (NA), Italy</p>	
<i>Evaluation facility</i>	<p><b>SERMA TECHNOLOGIES</b> 14 rue Galilee, CS 10055, 33615 Pessac, France</p>	
<i>Recognition arrangements</i>	<p><b>CCRA</b></p> 	<p><b>SOG-IS</b></p> 
<b>The product is recognised at EAL4 level.</b>		

# 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](http://www.ssi.gouv.fr).



# Contents

<b>1. THE PRODUCT .....</b>	<b>6</b>
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. PRODUCT DESCRIPTION.....	6
1.2.1. <i>Introduction</i> .....	6
1.2.2. <i>Product identification</i> .....	6
1.2.3. <i>Security services</i> .....	7
1.2.4. <i>Architecture</i> .....	7
1.2.5. <i>Life cycle</i> .....	8
1.2.6. <i>Evaluated configuration</i> .....	9
<b>2. THE EVALUATION.....</b>	<b>10</b>
2.1. EVALUATION REFERENTIAL .....	10
2.2. EVALUATION WORK .....	10
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS ACCORDING TO ANSSI'S TECHNICAL REFERENTIAL .....	10
2.4. RANDOM NUMBER GENERATOR ANALYSIS .....	10
<b>3. CERTIFICATION.....</b>	<b>11</b>
3.1. CONCLUSION .....	11
3.2. RESTRICTIONS .....	11
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
<b>ANNEX 1. EVALUATION LEVEL OF THE PRODUCT... ERREUR ! SIGNET NON DEFINI.</b>	
<b>ANNEX 2. EVALUATED PRODUCT REFERENCES .....</b>	<b>13</b>
<b>ANNEX 3. CERTIFICATION REFERENCES .....</b>	<b>16</b>

# 1. The product

## 1.1. Presentation of the product

The evaluated product is the smart card « SOMA-c003 – EAC, SAC and AA applications, version 1.3» developed by Arjowiggins Security SAS – Gep S.p.A. on the microcontroller ST23R160 (and the commercial derivatives ST23R80A and ST23R48A) manufactured by STMicroelectronics.

The evaluated product is a contactless smart card. It implements the travel document features according to the specifications from International Civil Aviation Organization. This product is designed to check the authenticity of the travel document, and to identify its holder during a border control, with the support of an inspection system.

## 1.2. Product description

### 1.2.1. Introduction

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

The security target claims strict conformance to [PP EAC] and [PP PACE] protection profiles.

### 1.2.2. Product identification

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

The certified version of the product can be identified by the response to the GET DATA command (see [GUIDES]).

The certified version of the product can be identified as well by the following elements:

Configuration		Source
TOE commercial name	SOMA Electronic Passport with EAC	Arjowiggins Security SAS – Gep S.p.A.
Product reference (internal label)	SOMA-c003_1_3	Arjowiggins Security SAS – Gep S.p.A.
Product reference (IC label)	ST23R160/80A/48A	Arjowiggins Security SAS – Gep S.p.A.
Operating System reference	SOMA	Arjowiggins Security SAS – Gep S.p.A.
HEX file reference	-SOMA-c003_1_3_DLV_02.dlv (ROM code) -SOMA-c003_1_3_DLV_02.dlv (EEPROM code)	Arjowiggins Security SAS – Gep S.p.A.
IC identification	ST23R160	STMicroelectronics

IC reference	ST23R160BQFM	STMicroelectronics
ROM code version	1.0	Arjowiggins Security SAS – Gep S.p.A.

### 1.2.3. Security services

The TOE provides mainly the following evaluated security services:

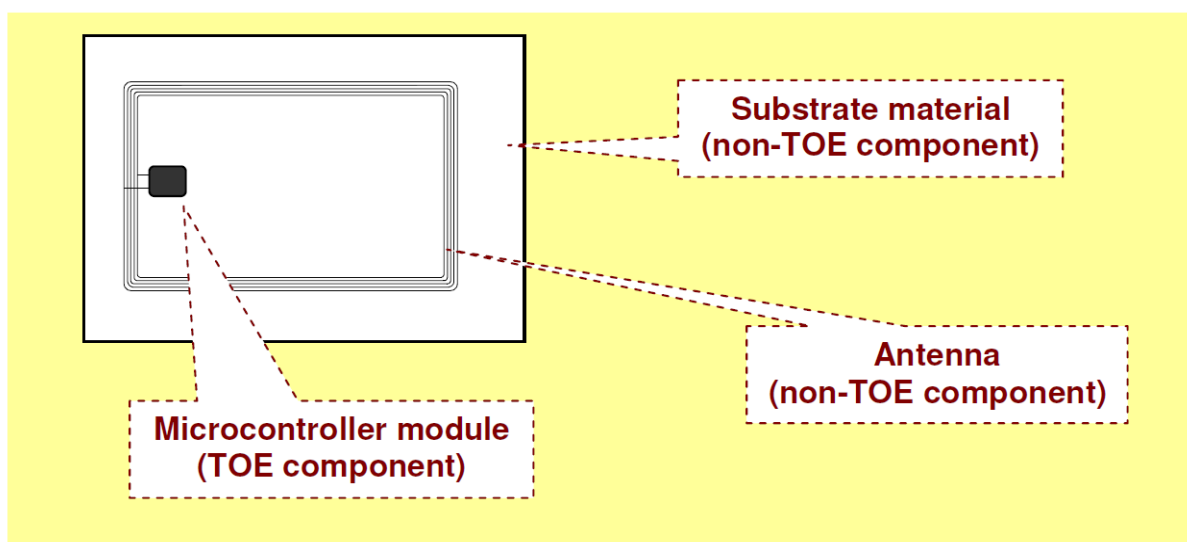
- protection of integrity of the holder's data stored on the card: issuing state or organization, travel document number, expiration date, holder's name, nationality, birth date, sex, holder's face portrait, additional biometric data, data for managing the security of the document and other optional data;
- access control to holder's data stored on the card;
- authentication between the travel document holder and the inspection system prior to any border control by the SAC mechanism;
- integrity and confidentiality of data read by the *Secure Messaging* mechanism;
- authentication of the microcontroller by the optional AA mechanism ("Active Authentication");
- strong authentication between the microcontroller and the inspection system by the EAC mechanism (Extended Access Control) prior to any access to biometric data.

### 1.2.4. Architecture

The product is a smart card consisting of:

- the ST23R160 revision B microcontroller, developed and produced by STMicroelectronics;
- the operating system SOMA developed by Arjowiggins Security SAS – Gep S.p.A.;
- The MRTD application developed by Arjowiggins Security SAS – Gep S.p.A.;

The physical architecture of the product is summed up by the following picture:



The software components are divided into a set of subsystems:

- Hardware Abstraction Layer (HAL) Management;
- Commands Management;
- Security Management;

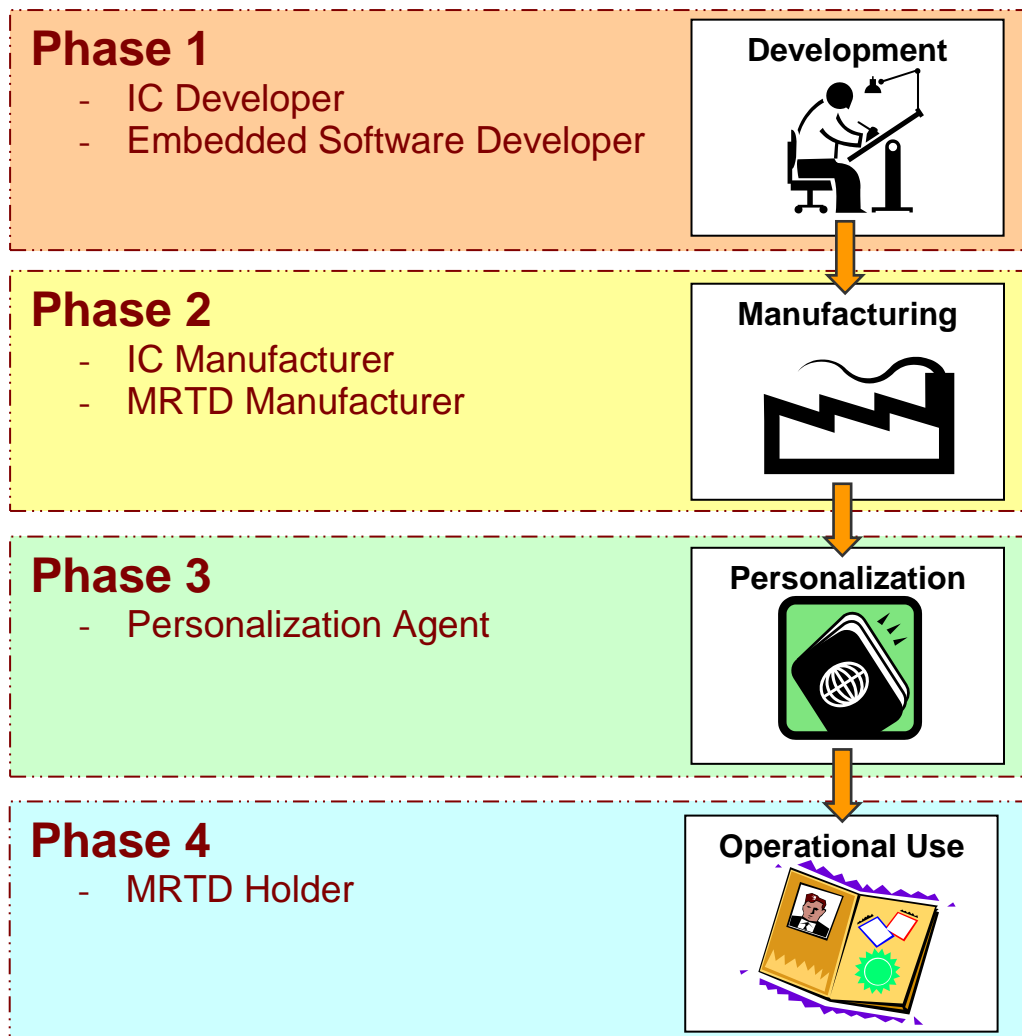
- Data object and Non Volatile Memory (NVM) Management;
- Communication Management;
- Initialization and Card Management;
- Patch Management.

These components are programmed on the IC ST23R160, included in the TOE.

### 1.2.5. Life cycle

The product’s life cycle is organised as follows:

- development phase (phase 1);
- manufacturing phase (phase 2);
- personalization phase (phase 3);
- operational use phase (phase 4).







The software components of the product have been developed on the following site:

**Arjowiggins Security SAS – Gep S.p.A.**

Viale Remo De Feo 1,  
80022 Arzano (NA),  
Italy

The microcontroller has been developed and manufactured by STMicroelectronics on its site (see [ANSSI-CC-2012/77]).

The « product administrators » are the states or organisations issuing the travel document.  
The « product users » are the travellers and the inspection systems during the operational use phase.

***1.2.6. Evaluated configuration***

The certificate applies to the the product presented in section 1.2.1. The evaluation applies only to the configuration including the following mechanisms:

- « Extended Access Control »;
- « Supplemental Access Control »;
- « Active Authentication ».

## 2. The evaluation

### 2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 4** [CC] and with the evaluation methodology defined in the CEM manual [CEM].

For assurance components which are not covered by [CEM] manual, the evaluation facility own evaluation methods and validated by ANSSI, have been used.

In order to meet the specificities of smart cards, the [JIWG IC] and [JIWG AP] guides have been applied. Thus the AVA\_VAN level has been determined according to the rating table of the [JIWG AP] guide. For memory, this rating table is more demanding than the default one defined in the standard method [CC], used for other types of products (software products for example).

### 2.2. Evaluation work

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

This evaluation has taken into account the results of the evaluation of the microcontroller « ST23R160 » at EAL6 level augmented by the component ALC\_FLR.1, compliant with the [PP0035] protection profile. This microcontroller has been certified the 8<sup>th</sup> of November 2012 under the reference [ANSSI-CC-2012/77].

The level of resistance of the microcontroller has been confirmed the 4<sup>th</sup> of December 2013 within the surveillance process, see [SUR\_IC].

The evaluation technical report [ETR], delivered to ANSSI the 12<sup>th</sup> of June 2014, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “pass”.

### 2.3. Cryptographic mechanisms robustness analysis according to ANSSI’s technical referential

The robustness of cryptographic mechanisms according to the ANSSI’s technical referential [REF\_CRY] has not been analyzed. Nevertheless, the evaluation has not lead to the identification of any design and implementation vulnerabilities for the aimed AVA\_VAN level.

### 2.4. Random number generator analysis

The random number generator of the product was out of the scope of the evaluation and has not been analyzed. The random number generator used by the final product, however, was evaluated within the evaluation of the microcontroller (see [ANSSI-CC-2012/77]).

## 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 « SOMA-c003 – EAC, SAC and AA applications, version 1.3» submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented by the component ALC\_DVS.2, ATE\_DPT.2 and AVA\_VAN.5.

### 3.2. Restrictions

This certificate only applies on the product specified in section 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 provided 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 recognition agreement made by SOG-IS in 2010 allows recognition from Signatory States of the agreement<sup>1</sup>, of the 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].

---

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

The «Common Criteria Recognition Arrangement» allows the recognition, by signatory countries<sup>2</sup>, 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:



---

<sup>2</sup> 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. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	2	2	Testing: security enforcing modules
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

## Annex 2. Evaluated product references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> <li>- Security Target SOMA-c003 electronic passport EAC-SAC-AA, reference: TCAE130012, version 1.1, 28<sup>th</sup> May 2014, edited by Arjowiggins Security SAS – Gep S.p.A.</li> </ul> <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> <li>- Security Target SOMA-c003 electronic passport EAC-SAC-AA, reference: TCAE140024, version 1.1, 29<sup>th</sup> April 2014, edited by Arjowiggins Security SAS – Gep S.p.A.</li> </ul>
[ETR]	<p>Evaluation technical report :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report – SOMA-c003 electronic passport, reference SOMA-c003_ETR_V1.0, version 1.0, 12<sup>th</sup> June 2014, edited by Serma Technologies.</li> </ul>
[CONF]	<p>Configuration list :</p> <ul style="list-style-type: none"> <li>- Configuration List for SOMA-c003 electronic passport, reference TCAE140005, version 1.1, 29<sup>th</sup> May 2014, edited by Arjowiggins Security SAS – Gep S.p.A.</li> </ul>
[GUIDES]	<p>Administration guidance:</p> <ul style="list-style-type: none"> <li>- Personalization Guidance for SOMA-c003 Electronic passport, reference TCAE130018, version 1.3, 28<sup>th</sup> May 2014, edited by Arjowiggins Security SAS – Gep S.p.A.;</li> <li>- Pre-Personalization Guidance for SOMA-c003 Electronic passport, reference TCAE130017, version 1.4, 28<sup>th</sup> May 2014, edited by Arjowiggins Security SAS – Gep S.p.A..</li> </ul> <p>User guidance:</p> <ul style="list-style-type: none"> <li>- User Guidance for SOMA-c003 Electronic passport, reference TCAE130019, version 1.2, 28<sup>th</sup> May 2014, edited by Arjowiggins Security SAS – Gep S.p.A..</li> </ul>
[ANSSI-CC-2012/77]	<p>« Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1, référence : maskset K2V0A, révision interne B »  <i>Certified the 8<sup>th</sup> of November 2012 under the reference ANSSI-CC-2012/77.</i></p>
[SUR_IC]	<p>« ST23R160B &amp; produits derives »  <i>Surveillance report of 4<sup>th</sup> of December 2013 under the reference ANSSI-CC-2012/77-S01.</i></p>
[PP EAC]	<p>Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control, version 1.3.2, 5<sup>th</sup> December 2012. <i>Certified by BSI (Bundesamt für Sicherheit in der</i></p>



	<i>Informationstechnik) under the reference BSI-PP-0056-V2-2012-MA-02.</i>
[PP PACE]	Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.0, 10 <sup>th</sup> November 2011. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0068-V2-2011.</i>
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.</i>

### 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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional requirements, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance requirements, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, revision 4, ref CCMB-2012-09-004.
[JIWG IC]*	Mandatory Technical Document – The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]*	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9 January 2013.
[COMP]*	Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, version 1.2, January 2012..
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 <sup>th</sup> January 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 dated 26 <sup>th</sup> January 2010 attached to the Référentiel général de sécurité (RGS_B_1), cf. www.ssi.gouv.fr

\*SOG-IS document ; in the CCRA recognition scope, the equivalent CCRA supporting document is applied.