



PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

## **Certification Report ANSSI-2009/14**

**Passeport MorphoePass EAC CC with BAC,  
AA and EAC RSA or EAC ECC, on  
STMicroelectronics ST19NR66-A/1.1.0**

*Paris, 23<sup>rd</sup> 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](mailto:certification.dcssi@sgdn.gouv.fr)

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

<i>Certification report reference</i>	<b>ANSSI-2009/14</b>	
<i>Product name</i>	<b>Passeport MorphoePass EAC CC with BAC, AA and EAC RSA or EAC ECC, on STMicroelectronics ST19NR66- A/1.1.0</b>	
<i>Product reference</i>	<b>MORPHOEPASSCC/ST19NR66-A/1.1.0</b>	
<i>Protection profile conformity</i>	<b>[PP EAC]</b> <b>Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control</b>	
<i>Evaluation criteria and version</i>	<b>Common Criteria version 2.3</b> <b>compliant with ISO 15408:2005</b>	
<i>Evaluation level</i>	<b>EAL 4 augmented</b> <b>ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4</b>	
<i>Developers</i>	<b>Sagem Sécurité SA</b> Etablissement d’Osny, 18 Chaussée Jules César, 95520 Osny, France	<b>STMicroelectronics</b> Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France
<i>Sponsor</i>	<b>Sagem Sécurité SA</b> Etablissement d’Osny, 18 Chaussée Jules César, 95520 Osny, France	
<i>Evaluation facility</i>	<b>CEA - LETI</b> 17 rue des martyrs, 38054 Grenoble Cedex 9, France Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr	
<i>Recognition arrangements</i>	<b>CCRA</b> 	<b>SOG-IS</b> 
	<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, 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](http://www.ssi.gouv.fr).

# Content

<b>1. THE PRODUCT .....</b>	<b>6</b>
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION .....	6
1.2.1. <i>Product identification</i> .....	7
1.2.2. <i>Security services</i> .....	7
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Life cycle</i> .....	9
1.2.5. <i>Evaluated configuration</i> .....	10
<b>2. THE EVALUATION.....</b>	<b>11</b>
2.1. EVALUATION REFERENTIAL .....	11
2.2. EVALUATION WORK .....	11
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	11
<b>3. CERTIFICATION.....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS.....	12
3.3. RECOGNITION OF THE CERTIFICATE.....	12
3.3.1. <i>European recognition (SOG-IS)</i> .....	12
3.3.2. <i>International common criteria recognition (CCRA)</i> .....	13
<b>ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....</b>	<b>14</b>
<b>ANNEX 2. EVALUATED PRODUCT REFERENCES .....</b>	<b>15</b>
<b>ANNEX 3. CERTIFICATION REFERENCES .....</b>	<b>17</b>

# 1. The product

## 1.1. Presentation of the product

The evaluated product is Morpho ePass EAC CC with BAC, AA & EAC RSA or EAC ECC software, developed by Sagem Sécurité SA, embedded in the secure microcontroller ST19NR66-A Rev. C, developed and manufactured by STMicroelectronics.

The evaluated product is a contactless smart card with its antenna. It's an ICAO compliant eTravel document. It is a contactless microcontroller with embedded software dedicated to authenticate the eTravel document and to identify its owner at borders controls, using an inspection system, in charge of:

- The integrity protection of the eTravel document's holder sensitive data: country or issuance organization, travel document number, expiration date, holder name, birth date, gender, user's facial picture, optional data, additional holder's biometric data and various information dedicated to document enforcing security;
- eTravel document user's authentication and inspection system's authentication (document's reader) before any border control operation, using Basic Access Control mechanism;
- User's data integrity and confidentiality protection, during the reading process using the secure messaging mechanism;
- Authentication of the hardware chip using Active Authentication function (if activated, if not, chip authentication will be done);
- Strong chip and reader authentication before any attempt to read biometric data via the Extended Access Control mechanism.

The product is also providing eServices dedicated to eAdministration, such as Identification, Authentication & Signature (IAS), in full conformance with the specifications of the common platform for eAdministration, but these eServices are outside the scope of the evaluation.

The microcontroller is also providing a contact interface allowing the final product to be used with the contact interface.

This chip and its embedded software are to be inserted in a regular passport's cover. This could be done using modules or inlays. The final product could be an ePassport, a smart card, or use different other form factors.

## 1.2. Evaluated product description

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

This security target conforms to [PP EAC] protection profile.

### **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 & version: MorphoEpassCC version 1.1.0;
- Microcontroller name & version: ST19NR66-A en version C;
- Platform identification: MORPHOEPASSCC/ST19NR66-A/1.1.0.

All those data can be checked by the CPLC data, as indicated in the Configuration management plan (cf. [CONF]).

### **1.2.2. Security services**

The product mainly provides the following security services:

- Authentication: Personalization user authentication, BAC authentication, "Active Authentication", "Chip Authentication", "Terminal Authentication";
- Cryptography: ECDSA, RSA, ECDH, DH, TDES, Retail MAC, SHA;
- « Secure Messaging » with BAC & EAC;
- Sensitive data access control;
- Crypto-Keys secure management;
- Life cycle management;
- Embedded applications separation;
- Safe state control for embedded applications;
- Protection against attacks.

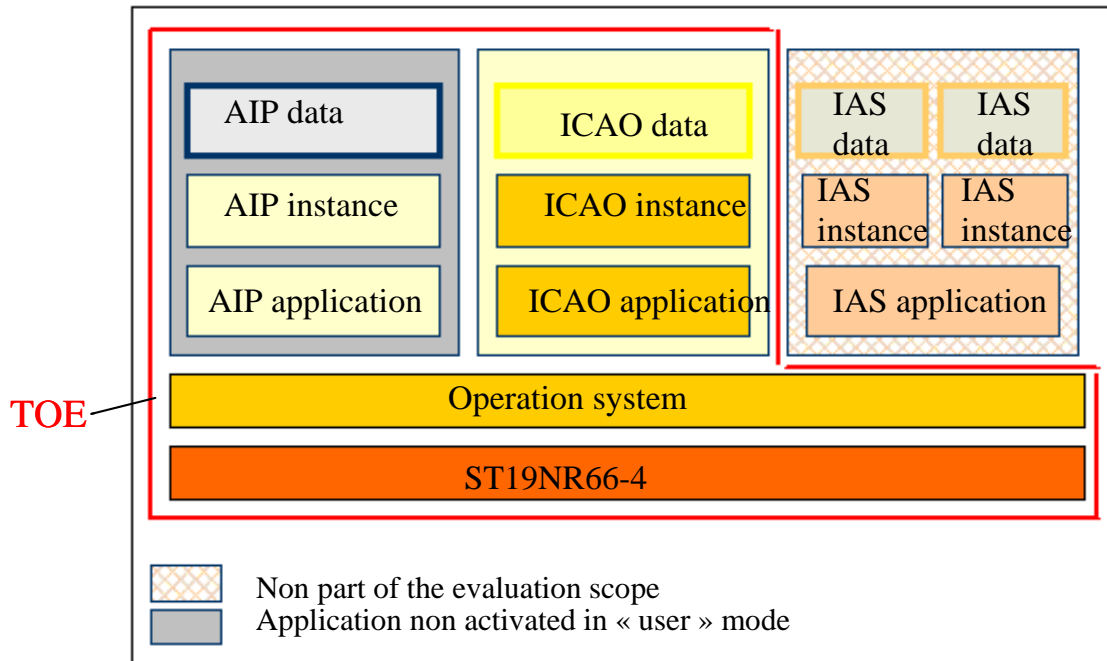
The security services provided by the hardware microcontroller are described in the chip certification report (cf. [2007/23]).

### **1.2.3. Architecture**

The product is based on a microcontroller, an embedded operating system and three applications:

- AIP dedicated to product's personalization process, deactivated in user phase;
- ICAO application for services management during the regular use phase;
- IAS for eAdministration during the use phase that could be instantiated several times (the applet code in ROM is unique, it addressed data which can be changed for the various applications' instances); the IAS application is outside the scope of the evaluation.

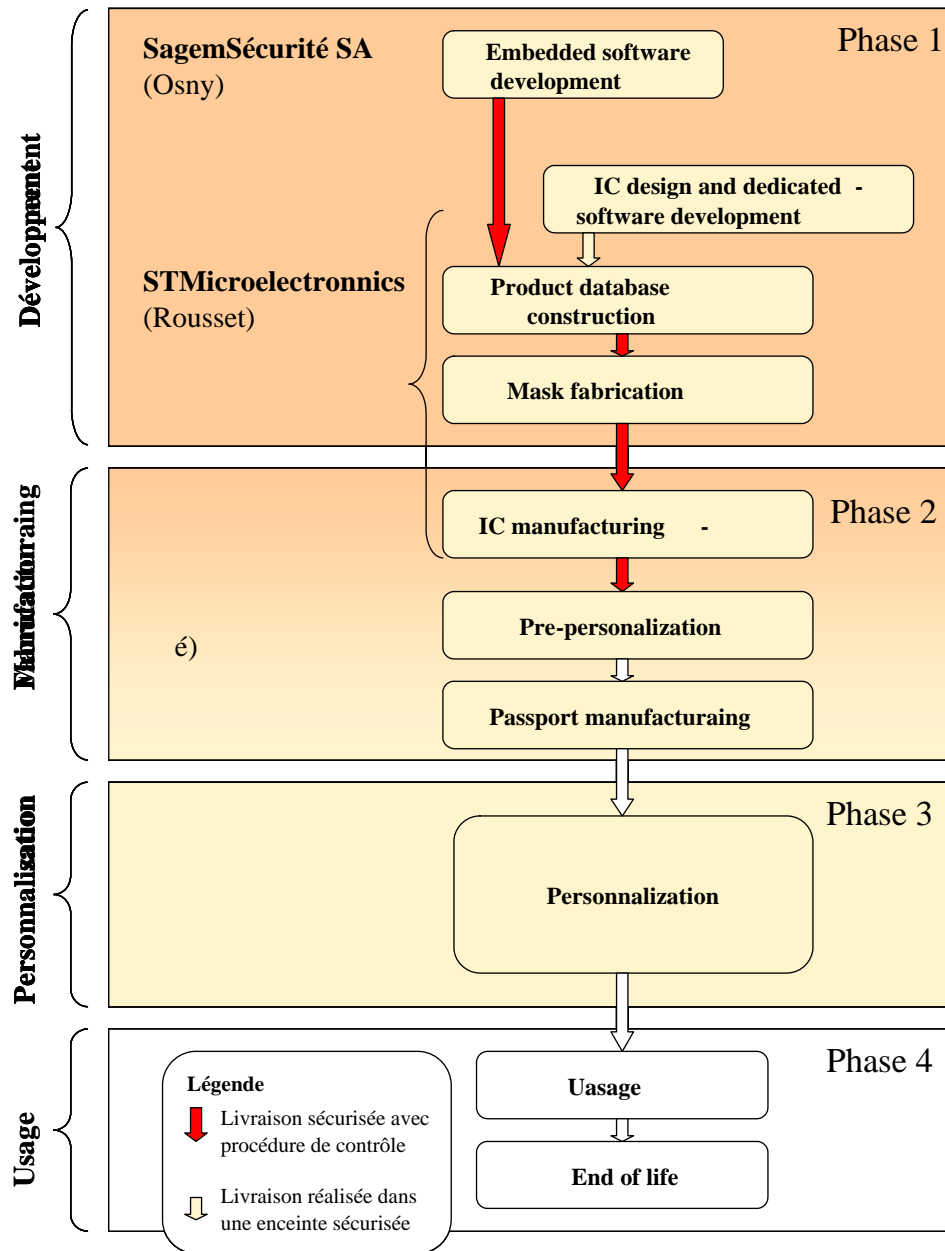
The following picture sums up the product architecture:





### 1.2.4. Life cycle

The product's life cycle is organized as follow:



The software has been developed on the following site :

**Sagem sécurité SA**

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

The microcontroller has been developed and manufactured by STMicroelectronics on the following site:

**STMicroelectronics**

Smartcard IC division, ZI de Rousset, BP2,  
13106 Rousset Cedex,  
France

The manufacturing phase for the eTravel document (Pre-Personalization) could be performed by STMicroelectronics or by a contractor. This phase, out of the evaluation scope, is addressed by the guidance (cf. [GUIDES]).

The inlays and eTravel document covers' manufacturing phases are not part of the evaluation, they are considered without impact on platform's security because the product is protected during these phases.

***1.2.5. Evaluated configuration***

The evaluated product is a generic ePassport platform, which could be personalized via several configurations. The certificate applies to the following configurations:

- Basic Access Control;
- Extended Access Control with RSA or ECC ;
- Active Authentication.

IAS Application is out of the evaluation perimeter as none of associated data are identified in the ST as sensitive data to be protected by the product. Anyway, as an embedded application, it has been taken into account by the evaluation process, especially for the vulnerability assessment.

The antenna and the eTravel document manufacturing phase are not included in the evaluation scope.

## 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].

For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS 34], validated by DCSSI, 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 [COMP] 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 “ST19NR66-A version C” at EAL5 level augmented with ALC\_DVS.2, AVA\_MSU.3 and AVA\_VLA.4, compliant with the [PP/9806] and [PP0002] protection profiles have been used. This microcontroller has been certified by DCSSI (cf. [2007/23]).

The microcontroller robustness level has been confirmed on 11 March 2008 in a surveillance process (Cf. N°483/SGDN/DCSSI/SDR).

The evaluation relies on evaluation results related to:

- Sagem Sécurité development environment, evaluated on July 2008 under the control of BSI<sup>1</sup> with satisfactory results (This will be stated in a BSI report BSI-DSZ-CC-0449 in an on going project);
- The previous version of the product also certified by DCSSI (cf. [DCSSI-2008\_23]).

The evaluation technical report [ETR], delivered to DCSSI the 19 March 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 analyzed by DCSSI on the previous version of the product (which has been certified by DCSSI (cf. [DCSSI-2008\_23]) during DCSSI qualification process (cf. [DCSSI-QS\_1979]).

---

<sup>1</sup> Bundesamt für Sicherheit in der Informationstechnik

## 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 MorphoePass EAC CC with BAC, AA & EAC RSA or EAC ECC, developed by Sagem Sécurité SA and embedded in the microcontroller ST19NR66-A Rev. C, developed by STMicroelectronics, submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL4 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].

### 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<sup>1</sup>, 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:



---

<sup>1</sup> 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<sup>1</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>1</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, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

## Annex 1. Evaluation level of the product

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
ACM Gestion de configuration	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	2	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	1	1	1	2	3	3	4	2	Fully defined external interfaces
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	2	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	1	Informal TOE security policy model
AGD Guides d'utilisation	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 Support au cycle de vie	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	1	Testing: high-level 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
AVA Estimation des vulnérabilités	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Analysis and testing for insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

## Annex 2. Evaluated product references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"><li>- Security Target: Morpho-ePass V3, reference SK 00000 63506, version 1.6, 29/08/08,</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 - MorphoePass EAC CC - Public Version, reference SSE-0000070468, version 1.2,</li></ul>
[RTE]	<p>Evaluation technical report :</p> <ul style="list-style-type: none"><li>- ré-évaluation HELIOS, reference LETI.CESTI.HEL.RTE.002, version 1.0, 18/03/09, CESTI LETI</li></ul>
[CONF]	<p>Configuration list:</p> <ul style="list-style-type: none"><li>- Plan de gestion de configuration logiciel, reference SK 0000066065, version 1.1, 06/06/07,</li><li>- Fiche de Version du Logiciel MorphoEpassCC 1.1.0 Cible ST19NR66-A, reference SSE-0000067783, version 1.2, 06/02/09,</li></ul>
[GUIDES]	<p>Installation guidance:</p> <ul style="list-style-type: none"><li>- Documentation d'installation, de génération et de démarrage, reference SSE-0000068096, version 1.1, 10/01/08,</li></ul> <p>Administration guidance:</p> <ul style="list-style-type: none"><li>- Procédures de livraison Fondateur ST Microelectronics, reference SSE-0000067784, version 1.1, 29/11/07,</li><li>- ICAO Application Pre-personalisation manual, reference SSE-0000070088, version 1.2, 17/06/08,</li><li>- ICAO Application Personalisation manual, reference SSE-0000067414, version 1.2, 17/06/08,</li></ul> <p>User guidance:</p> <ul style="list-style-type: none"><li>- ICAO Application User manual, reference SSE-0000067415, version 1.2, 17/06/08,</li></ul>

[2007/23]	DCSSI certificate issued on 13 December for ST19NR66-A Secure Microcontroller. <i>Certified by DCSSI under the reference 2007/23</i>
[DCSSI-2008_23]	DCSSI certificate issued on 28 July 2008 for the passport product Morpho-ePass V3 with BAC, AA and EAC RSA or EAC ECC, on STMicroelectronics IC. <i>Certified by DCSSI under the reference DCSSI-2008/23.</i>
[DCSSI-QS_1979]	DCSSI qualification, standard level, issued on 15 September 2008, under 1979/SGDN/DCSSI reference, for the passport product Morpho-ePass V3 on ST19NR66-A révision C microcontroller, for its AA and EAC mechanisms, along with conditions on ECC and RSA key length due a passport type product lifetime.
[OACI]	ICAO Doc 9303, Sixth Edition, 2007
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. <i>Certified by DCSSI under the reference PP/9806.</i>
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.</i>
[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2, 19 November 2007. <i>Certifier by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0026</i>



## Annex 3. Certification references

Decree number 2002-535 dated 18 <sup>th</sup> 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 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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik