PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2007/24

E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller

Paris, 14th of December 2007

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 DCSSI (Central Directorate for Information Systems Security), 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
Direction Centrale 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.pm.gouv.fr

Certification report reference

DCSSI-2007/24

Product name

E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller

Product reference

Reference of the application: SPEC5 V014
Reference of the microcontroller with embedded software: ST19WR66I PQH

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

ACM_SCP.3, ADV_IMP.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, AVA_VLA.3

Developers

NTTDATA Corporation

Toyosu Center Bldg Annex, 3-3-9 Toyosu, Koto-ku, Tokyo 135-8671, Japan

STMicroelectronics

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

Sponsor

NTTDATA Corporation

Toyosu Center Bldg Annex, 3-3-9 Toyosu, Koto-ku, Tokyo 135-8671, Japan

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Phone: +33 (0)5 57 26 08 75, email : e.francois@serma.com

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, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department 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 principals 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 e-Passport (MRTD) configuration of the Xaica-Alpha64K platform developed by NTTDATA Corporation, embedded on the ST19WR66I secure microcontroller developed and manufactured by STMicroelectronics.

The evaluated product is a contactless smartcard with its antenna. The smartcard implements the e-Passport features according to the specifications from the International Civil Aviation Organization (cf. [ICAO]). The product enables:

- To store passport holder's signed data (issuing state or organization, passport number, expire date, holder's name, nationality, birth date, sex, other optional data) a holder's biometric data (face portrait), optional authentication data and several other pieces of data for managing the document security;
- To check passport's authenticity and to identify its holder during a boarder control with the support of an inspection system.

The chip and its embedded software are intended to be inserted into the cover page of traditional passport booklets.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.
The security target is based on the protection profile "Machine Readable Travel Document with ICAO Application, Basic Access Control" (cf. [PP MRTD]).

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:

- Reference of the platform: SPEC5 V014;
- IC manufacturer reference of the product: PQH;
- Reference of the microcontroller: ST19WR66I.

This reference can be checked using the command:

- GET TRACEABILITY INF;
- REQUEST LABEL;
- GET DATA.

For more details, refer to the guidance "Xaica-alpha64K - Platform Specification" (cf. [GUIDES].

1.2.2. Security services

The product provides mainly the following security services:

- Identification and authentication;
- Access control;

- Cryptography;
- Life cycle management;
- Secure messaging;
- Session keys management;
- Key storage management;
- Security Policy management;
- Auto-tests;

There is in addition the microcontroller security services:

- Hardware initialisation & TOE attribute initialisation;
- TOE configuration switching and control;
- TOE logical integrity;
- Test of the TOE;
- Administrators authentication;
- Storage and Function Access Firewall;
- Physical tampering security function;
- Security violation administrator;
- Unobservability;
- Symmetric Key Cryptography Support;
- Asymmetric Key Cryptography Support;
- Unpredictable Number Generation Support.

1.2.3. Architecture

A microcontroller circuit embedding e-passport configuration of the Xaica-Alpha64K platform, including the holder's identification data is connected to an antenna and mounted on a plastic film. This "Inlay" is then embedded in the coversheet of the passport booklet and provides a contactless interface for the passport holder identification. This is represented in the following figure:

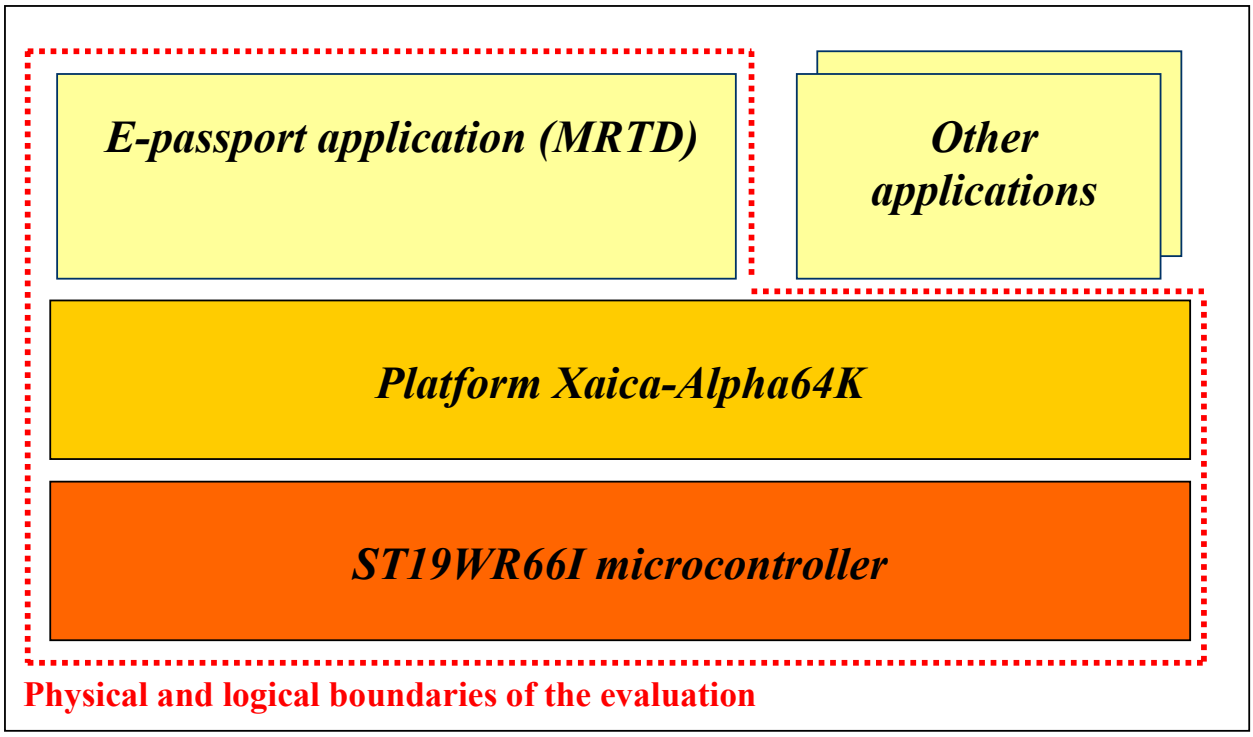

Figure 1 – Architecture of the product

The product provides the main following functionalities during its personalization and usage phases:

- Authentication mechanisms conformant to [ICAO] specification (Basic Access Control and Active Authentication);
- Personal passport holder and system related data storage and read access;
- Dedicated authentication mechanism compliant with Japanese government requirements allowing to personalize and to manage the application;
- Contactless interface (ISO14443 Type B);
- Smartcard application APDU commands set embedded and compliant with JICSAPV1.1 (equivalent to our ISO7816-3 and ISO7816-4).

1.2.4. Life cycle

The product's life cycle is organised as follow:

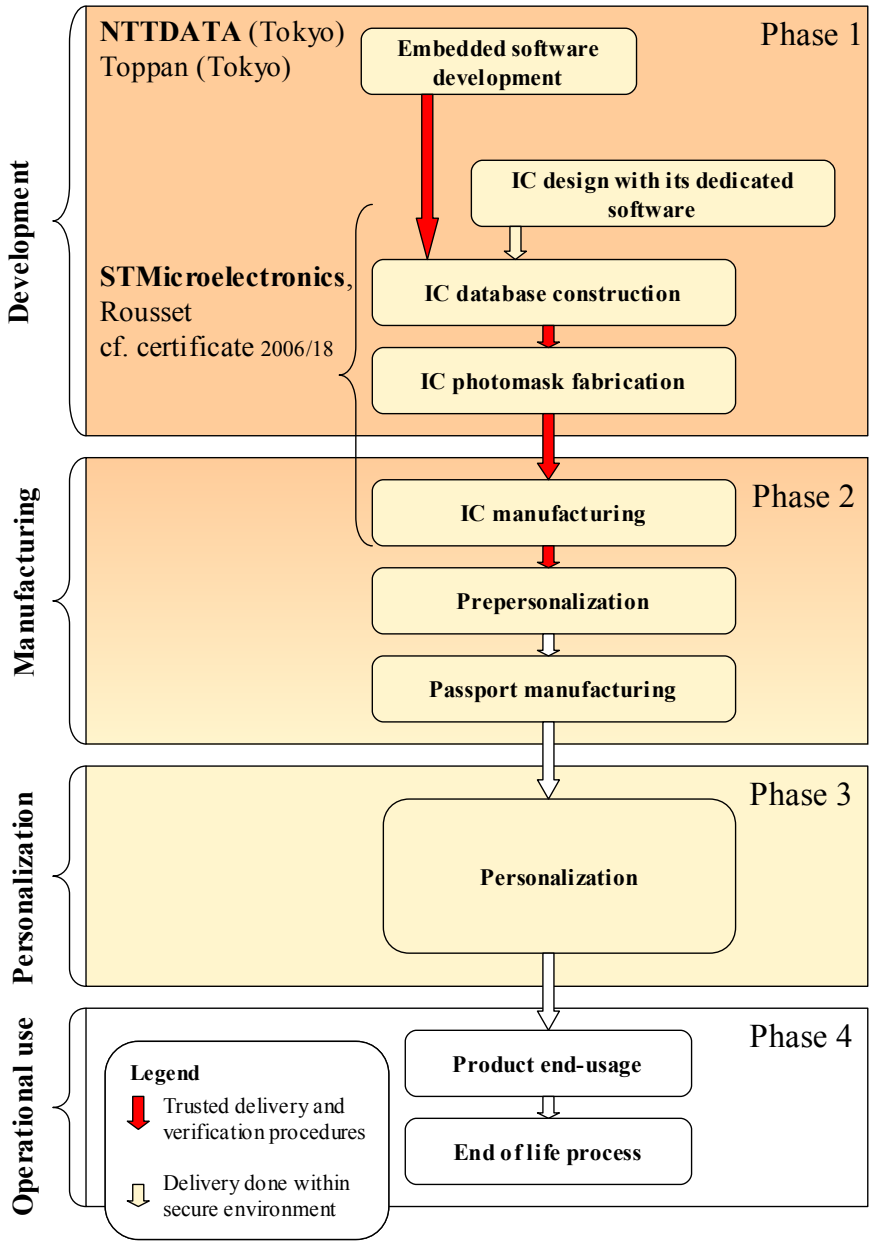

Figure 2 – Product life cycle

The platform has been developed by NTTDATA on the following site:

NTTDATA

Toyosu Center Building Annex,
3-3-9 Toyosu, Koto-ku,
Tokyo 135-8671, Japan

A part of the development was subcontracted to Toppan on the following site:

TOPPAN

Koishikawa building
1-3-3, Suido,Bunkyo-ku
Tokyo, Japan

The microcontroller is developed and manufactured by STMicroelectronics:

STMicroelectronics

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

The MRTD manufacturing phases (including pre-personalisation) are not in the scope of the evaluation. However, the secure pre-personalisation scheme provided by Developer was evaluated (cf. [GUIDES]).

1.2.5. Evaluated configuration

The certificate applies to the e-passport configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I microcontroller, as identified §1.2.1.
The Xaica-Alpha64K platform includes many other commands to address other needs (e.g. JUKI or Z applications). These commands are not usable because of the specific creation of the file structure that only deals with ICAO commands and are outside the scope of the evaluation.
The antenna and the MRTD manufacturing phase (booklet) are also not in the scope of the evaluation.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM]. For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS34], validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CCIC] and [CCAP] 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 is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "**ST19WR66I**" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] and [PP9806] protection profiles, have been used. This microcontroller has been certified the 7th of November 2006 under the reference 2006/18 (cf. [2006/18]).

The evaluation technical report [ETR], delivered to DCSSI the 11th of December 2007, 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 DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY] and have been taken into account in the evaluator vulnerability analysis.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality by 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 "E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller" 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], in particular:

- The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, to initialise, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.
- The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organization:
    - Establish the correct identity of the holder and create biographic data for the MRTD;
    - Enrol the biometric reference data of the MRTD holder i.e. the portrait;
    - Personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the Document Security Object and the Active Authentication Private Key). The Personalization Agents enable the Basic Access Control function of the TOE. The Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip;
- The Issuing State or Organization must:
    - Generate a cryptographic secure Country Signing Key Pair;
    - Ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment;
    - Distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity;

  The Issuing State or organization must:
    - Generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys;
    - Sign Document Security Objects of genuine MRTD in a secure operational environment only;

  - Distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object includes all data in the data groups DG1 to DG16 if stored in the LDS according to [ICAO];
- The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures in order to detect any manipulation of the physical MRTD.
- The border control officer of the Receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems.
- Additionally the Extended Inspection System shall perform the Active Authentication mechanism to verify the Authenticity of the presented MRTD's chip;
- The inspection system of the receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. For that purpose, the receiving State examining the logical MRTD will use inspection systems, which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data and implement the terminal part of the Active Authentication.
- The holder must not disclose the MRZ to any unauthorized people to prevent attempts to disclose the electronic data of the MRTD.
- The entropy of the printed MRZ data shall be kept 56bits as minimum for the VLA level targeted. The detailed calculation method is described in the guidance "Operator Manual for Personalization Agent" (cf. [GUIDES]).

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued 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:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

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

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, the Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States.

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
ACM Configuration management	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	3	Development tools CM coverage
ADO Delivery and operation	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 Development	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	3	Formal TOE security policy model
AGD Guidance	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 Life-cycle support	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	2	Standardized life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
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 Vulnerability assessment	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	2	Validation of analysis
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	3	Moderately resistant

Annex 2. Evaluated product references

[2006/18]	Certification report 2006/18 - ST19WR66I microcontroller, 7th of November 2006 SGDN/DCSSI
[ST]	Reference security target for the evaluation: - Xaica-alpha64K Security Target (ePassport configuration) Reference: NTTD-STep-XAICAALPHA64KST19, version 1.20, December 6, 2007 NTTDATA For the needs of publication, the following security target has been provided and validated in the evaluation: - Xaica-alpha64K Security Target Lite, Reference: NTTD-STL-XAICAALPHA64K-ST19, Version 1.00, December 14, 2007 NTTDATA
[ETR]	Evaluation Technical Report - ALPHA64K project, Reference: ALPHA64K_ETR_v1.2 Serma Technologies
[ANA-CRY]	Rapport d'analyse crypto N°902/SGDN/DCSSI/SDS/Crypto du 27 avril 2007 SGDN/DCSSI
[CONF]	Xaica-alpha64K - TOE Configuration List, Reference: NTTD-TCL-XAICAALPHA64K-ST19 v1.40 NTTDATA
[GUIDES]	- Xaica-alpha64K - Platform specification, Reference: NTTD-DD-XAICAALPHA64K-ST19 version 1.40 NTTDATA - Xaica-alpha64K - Procedure for OUTSOURCE issue data creation, Reference: NTTD-POS-XAICAALPHA64K-ST19 version 1.10 NTTDATA - Xaica-alpha64K - Manual for OUTSOURCE issue data creation, Reference: NTTD-MOS-XAICAALPHA64K-ST19 v1.20 NTTDATA - Xaica-alpha64K - Manual for delivery, installation and Issuance of OUTSOURCE, Reference: NTTD-DIO-XAICAALPHA64K-ST19 v1.20 NTTDATA - Operator Manual for MRTD manufacturer (booklet), Reference: NTTD-OMB-XAICAALPHA64K-ST19, version 1.10, NTTDATA

	- Operator Manual for Personalization Agent, Reference: NTTD-OMP-XAICAALPHA64K-ST19, version 1.30, NTTDATA - Operational Manual for User, Reference: NTTD-OMU-XAICAALPHA64K-ST19 version 1.10, NTTDATA
[ICAO]	- PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004 International Civil Aviation Organization, - Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004, International Civil Aviation Organization, - Machine Readable Travel Documents, supplement 9303, version 3.0, 12nd June 2005
[PP MRTD]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. *Certified under the reference BSI-PP-0017*
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certified by DCSSI under the reference PP/9806.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI under the reference BSI-PP-0002-2001.*

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, 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-2007-04-001 version 2.3, revision 1, April 2007.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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 with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR

[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