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-2011/21

PEACOS Electronic Passport with EAC on P5CD080 V0B, version 1.2

Paris, 1st July 2011

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-2011/21

Product name

PEACOS Electronic Passport with EAC on P5CD080 V0B

Product reference/version

PEACOS_NXP80_1_2 / Version 1.2

Protection profile conformity

[PP EAC], version 1.2
Machine Readable Travel Document with "ICAO Application", Extended Access Control

Evaluation criteria and version

Common Criteria version 3.1 revision 3

Evaluation level

EAL 4 augmented
ALC_DVS.2, AVA_VAN.5

Developers

Gep S.p.A
90 Corso Salvatore D'Amato, 80022 Arzano, Italy

NXP Semiconductors Germany GmbH
Box 54 02 40, D-22502 Hamburg, Germany

Sponsor

Istituto Poligrafico e Zecca dello Stato S.p.A
1027 Via Salaria , 00198 Roma, Italy

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, 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 « PEACOS Electronic Passport with EAC on P5CD080 V0B, reference PEACOS_NXP80_1_2 / Version 1.2 » developed by Gep S.p.A and NXP Semiconductors.

The evaluated product is a contactless smartcard. It implements the travel document features according to the specifications from the International Civil Aviation Organization (cf. [ICAO]). 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. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.
This Security target is compliant with the protection profile [PP EAC]. It is a demonstrable compliance.

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:
- commercial reference (Gep S.p.A) : PEACOS Electronic Passport, version 1.2;
- microcontroller's name and version (NXP): P5CD080 V0B;
- whole embedded software reference (Gep S.p.A): PEACOS_NXP80_1_2;
- NXP reference: P5CD080A4/T0B26350 (masked chip), PEACOS_FK03.hex (patch)..

The version of the product can be checked by the answer to the Get Data command on the "product identification data" (P1: 01h, P2: 10h):

50h 45h 41h 43h 4Fh 53h 5Fh 4Eh 58h 50h 38h 30h 5Fh 31h 5Fh 32h.

The data have the following meaning:
- OS identifier: 50h 45h 41h 43h 4Fh 53h 5Fh (PEACOS_);
- IC identifier: 4Eh 58h 50h 38h 30h 5Fh (NXP80_);
- OS version: 31h 5Fh 32h (1_);
- Patch version: 32h (2).

1.2.2. Security services

The TOE provides mainly the following evaluated security services:
- protection of integrity of the holder's stored data: 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;

- authentication between the travel document holder and the inspection system prior to any border control by the Basic Access Control mechanism;
- protection of integrity and confidentiality of data read by secure messaging;
- strong authentication of the chip and the inspection system prior to any biometric data retrieval by the Extended Access Control mechanism.

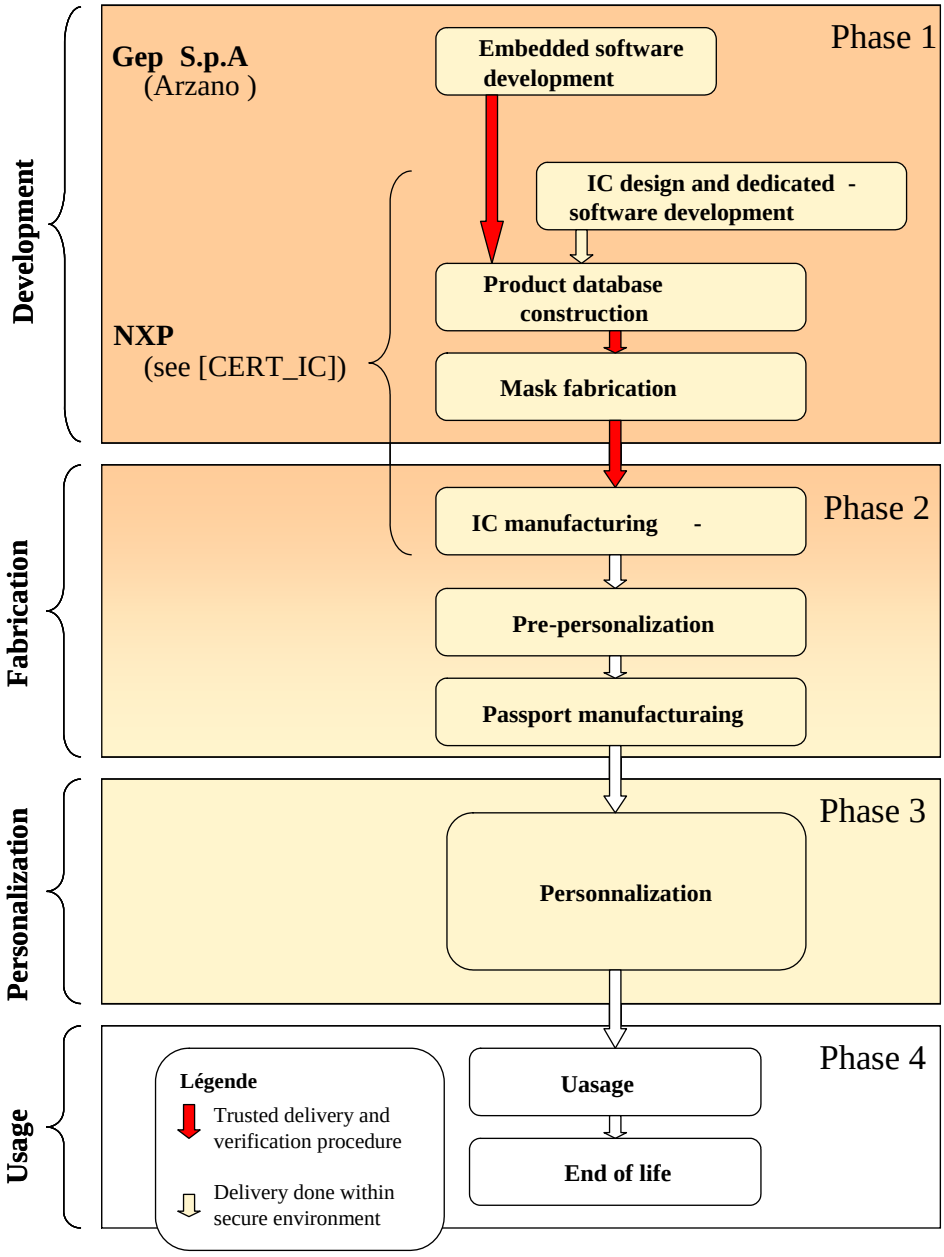
1.2.3. Architecture

The product consists of

- the P5CD080 V0B microcontroller, developed and produced by NXP ;
- the IC dedicaded software, developed by NXP;
- the software parts, developed by Gep S.p.A, which reference is PEACOS_NXP80_1_1, masked in the microcontroller's ROM, composed of:
    - the operating system (including the Hardware Abstraction Layer);
    - and the MRTD application;
- the software patch, developed by Gep S.p.A, which reference is PEACOS_FK03, loaded in the microcontroller's EEPROM.

1.2.4. Life cycle

The product's life cycle is organised as follow:



The embedded software has been developed on the following site:

Gep S.p.A

Corso Salvatore D'Amato, 90
80022 Arzano, Napoli
Italy

The microcontroller development sites are identified in the [CERT_IC] certification report.

1.2.5. Evaluated configuration

The certificate applies to the closed configuration of this product.
The product tested by the evaluation facility is typical to the final product (phase 7).

2. The evaluation

2.1. Evaluation referential

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

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 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 "P5CD080V0B" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile, have been used. This microcontroller has been certified the 3rd of November 2010 under the reference BSI-DSZ-CC-0680-2010 ([CERT_IC]).

The evaluation technical report [ETR], delivered to ANSSI the 6th of June 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 not been analysed regarding the ANSSI's technical referential. Nevertheless the evaluation has not lead 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 [CERT_IC] certification report). The evaluation has not lead to the identification of exploitable vulnerability for the aimed AVA_VAN level

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 "PEACOS Electronic Passport with EAC on P5CD080 V0B, version 1.2" 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, Italy, 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 Developmentt	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_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	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	**1**	**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	**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	**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**	Focused vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - "Security Target for the PEACOS Electronic Passport with Extended Access Control", reference TSRE090008, version 1.7. For the needs of publication, the following security target has been provided and validated in the evaluation: - "Security Target Lite for the PEACOS Extended Access Control MRTD" , reference TCLE100138, version 1.2.
[ETR]	"Evaluation Technical Report MATISSE Project", reference MATISSE_ETR_V1.2, version 1.2.
[CONF]	"Configuration Item List for the PEACOS Electronic Passport", référence TSRE100137, version 1.3.
[GUIDES]	Installation guidance: - "Initialization guidance for the PEACOS Electronic Passport", reference TSRE090016, version 1.2. Administration guidance: - "Personalization guidance for the PEACOS Electronic Passport", reference TSRE090017, version 1.2. User guidance: - "User Guidance for the PEACOS Electronic Passport", reference TSRE090011, version 1.1.
[CERT_IC]	Certification report for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated software. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-DSZ-CC-0680-2010.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.*
[PP EAC]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.2, 19th November 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0026-2006-MA-01.*

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, 8th January 2010, Management Committee.