PREMIER MINISTRE

Secretariat general for national Defence

Central Directorate for Information System Security

Certification Report DCSSI-2008/45

« eTravel EAC version 1.1 (version 01 02) on P5CD080 and P5CD144 microcontrollers »

Paris, 18th of December 2008

Courtesy Translation

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of the 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 product recommendation from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

All 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.gouv.fr

Certification report reference

DCSSI-2008/45

Products names

eTravel EAC v 1.1 80K (version 01 02) on P5CD080 microcontroller

and

eTravel EAC v1.1 144K (version 01 02) on P5CD144 microcontroller

Products references

on P5CD080 VOB : T1003327 version 1.1

and

on P5CD144 VOB : T1003883 version 1.1

protection profile conformity

BSI-PP-0026 version 1.2

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Developers

Gemalto SA

6 rue de la verrerie, 92197 Meudon, France

NXP Semiconductors GmbH

Box 54 02 40, D-22502 Hamburg, Germany

Sponsor

Gemalto SA

6 rue de la verrerie, 92197 Meudon, France

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

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

Recognition arrangements

CCRA

SOG-IS

These products are recognized 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 departement 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 certification procedures are available on the Internet site www.ssi.gouv.fr.

Table of content

1. The products

1.1. Presentation of the products

The evaluated products are "eTravel EAC v 1.1 (version 01 02) on P5CD080 and P5CD144 microcontrollers" developed by Gemalto and NXP Semiconductors, and manufactured by NXP Semiconductors.

These products are contactless smartcards with antenna. They implement the electronic travel document features according to the International Civil Aviation Organization specifications and to Extended Access Control. These are contactless microcontrollers with embedded software 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. They enable:

- Protection in integrity of the holder's data stored in the travel document: issuing state or organization, travel document number, expire date, holder's name, nationality, birth date, sex, holder's face portrait, optional information data, additional holder's biometric data and several other data for managing the document security;
- Authentication between the travel document holder and the inspection system (terminal reading travel documents) prior to any border control by means of the "Basic Access Control" mechanism;
- Protection in integrity and confidentiality of read data, by means of the "secure messaging" mechanism;
- Authentication of the chip by means of the Active Authentication mechanism (if it has been activated during pre-personalisation, at the request of the customer);
- Strong authentication of the chip and the inspection system prior to any biometric data retrieval, by means of the "Extended Access Control" mechanism.

These microcontrollers and their embedded software are intended to be inserted into the cover page of traditional passport booklets. They can be integrated into modules, inlays, or datapages. The final product can be a passport, a plastic card etc…

1.2. Evaluated products description

The security target [ST] defines the evaluated products, their evaluated security functionalities and their operational environment.
This security target is compliant to [PP EAC] protection profile.

1.2.1. Products identification

The configuration list [CONF] identifies the products constituent elements.
The certified version of these products can be identified by the following elements:

	Name	Reference	Version
On P5CD080 V0B	eTravel EAC v1.1 80K	T1003327	1.2
On P5CD144 V0B	eTravel EAC v1.1 144K	T1003883	1.2

These elements can be identified with the "GET DATA" command, as specified in the administration guide (cf. [GUIDES]) and in the configuration list (cf. [CONF]):

- For P5CD080 :
  - IC TYPE = **50 80**
  - OPERATING SYSTEM IDENTIFIER= **D0 00 67**
  - OPERATING SYSTEM RELEASE LEVEL= **01 02**

- For P5CD144 :
  - IC TYPE = **51 44**
  - OPERATING SYSTEM IDENTIFIER= **D0 00 68**
  - OPERATING SYSTEM RELEASE LEVEL**= 01 02**

1.2.2. Security services

The main security services provided by these products are:
- Reliability;
- Access control;
- Symmetric authentication mechanisms;
- Secure messaging;
- Chip authentication;
- Validity of the certificate chain;
- Asymmetric authentication mechanism.

The security services provided by the microcontrollers are:
- Random number generation;
- Triple DES coprocessor;
- AES coprocessor;
- Control of operating conditions;
- Protection against physical manipulation;
- Logical protection;
- Protection of mode control;
- Memory access control ;
- Special functions register access control.

1.2.3. Architecture

The product consists in the microcontroller, the embedded software comprising the tests and the commands and data management, and the logical data structure.

The following picture sums up the products architecture:

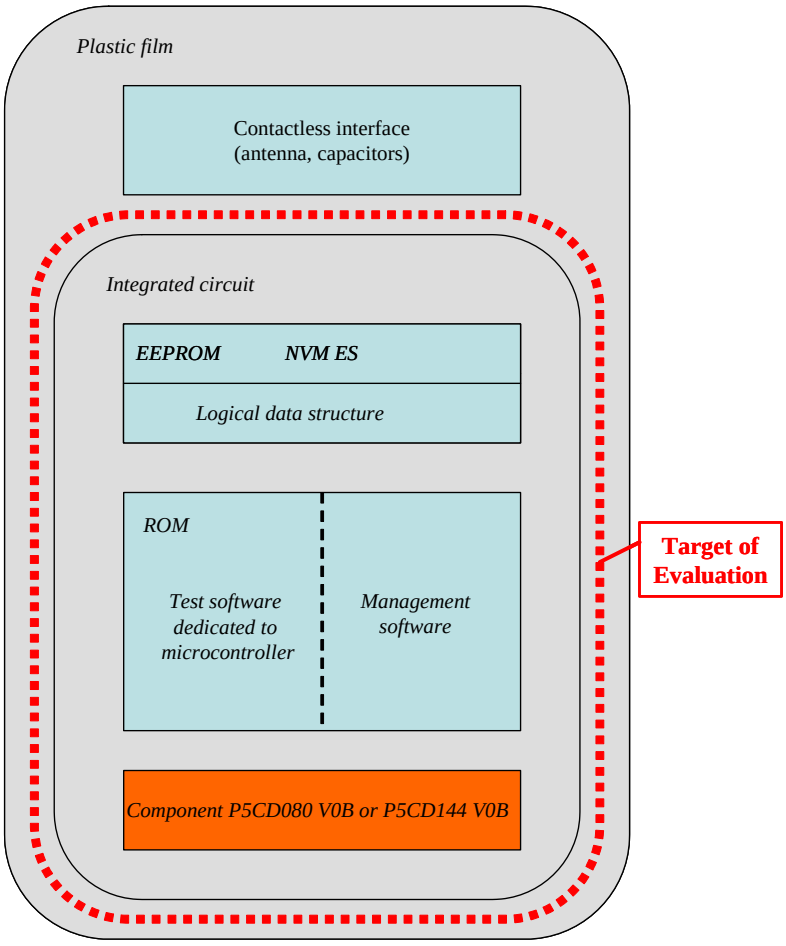

Figure 1 – Product architecture

1.2.4. Life cycle

The products life cycle is the following:

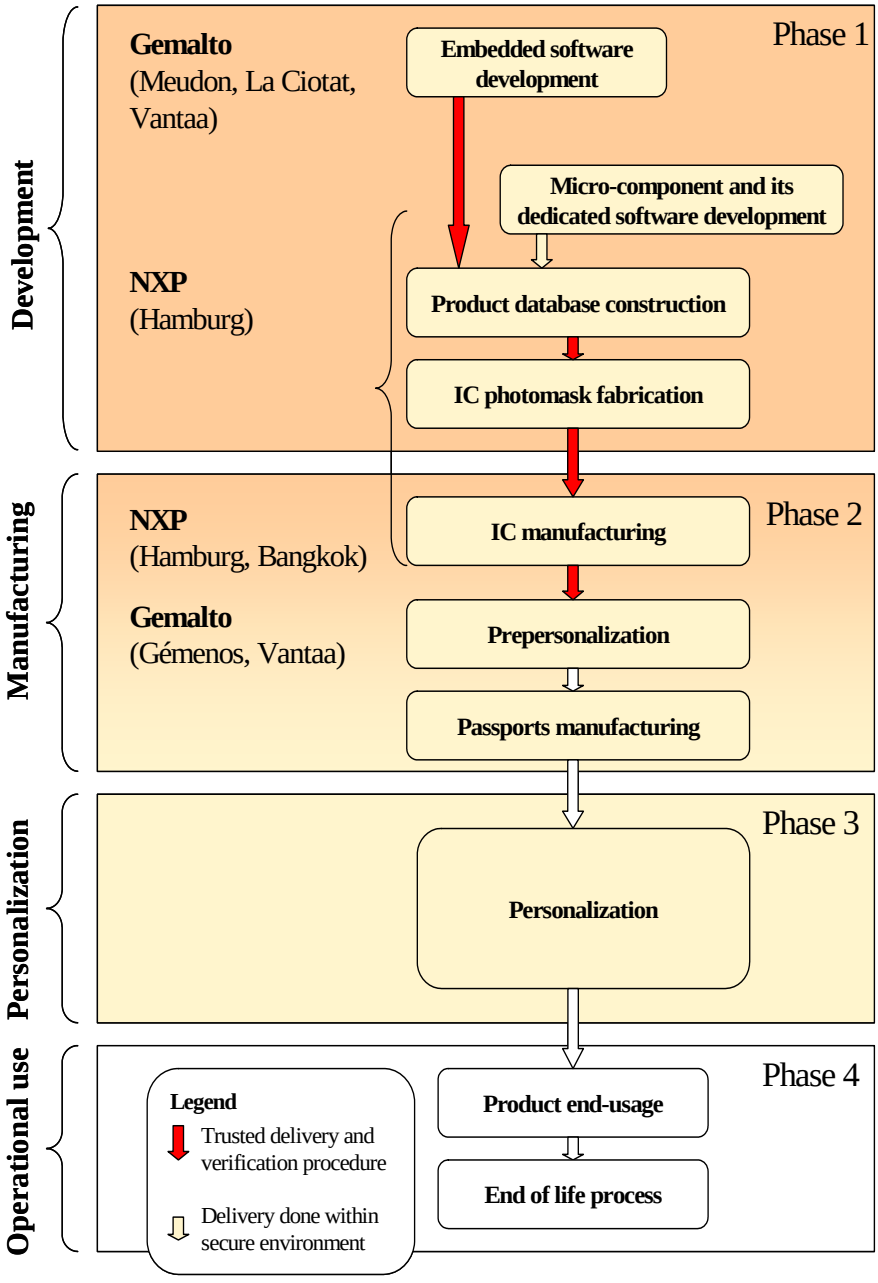

Figure 2 – Product Life-cycle

The products are developed on the following sites:

Gemalto

Turvalaaksonkaari 2
FI-01741 Vantaa
Finland

Gemalto

6 rue de la verrerie
92190 Meudon
France

Gemalto

Avenue du Jujubier
ZI Athelia IV
13705 La Ciotat
France

Gemalto

Avenue du Pic de Bretagne
13881 Gémenos
France

The microcontrollers are developed and manufactured by NXP Semiconductors on the following sites:

NXP Semiconductors

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

NXP Semiconductors

303 Chaengwattana Rd.,
Laksi Bangkok 10210,
Thailand

The «products administrators» are the travel document issuing states or organizations.
The «products users» are the travellers and the inspection systems during the usage phase.

1.2.5. Evaluated configuration

The evaluated products are generic e-Passport platform that can be personalized under different configurations. This certification report covers the configuration including the following mechanisms:

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

The antenna and the travel document manufacturing phase (booklet) are 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 [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 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 evaluations of the microcontrollers « P5CD080 V0B » and « P5CD144 V0B » at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with [PP0002] protection profile, have been used. The microcontrollers « P5CD080 V0B » and « P5CD144 V0B » have been certified on the 5th of July 2007 under the references BSI-DSZ-CC-0410-2007 and BSI-DSZ-CC-0411-2007.

The evaluation leans on the evaluation results of the "eTravel EAC v1.1 on P5CD080 and P5CD144 microcontrollers" product certified the 14th of August 2008 under the reference DCSSI-2008/28 [2008_28].

The evaluation technical report [ETR], delivered to DCSSI the 8th of August 2008, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

The evaluation technical report addendum [ETR_ADD], delivered to DCSSI the 25th of November 2008, provides details on the further work performed by the evaluation facility.

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 by the evaluator.

The analysed mechanisms reach the standard level defined in the DCSSI cryptographic referential (cf. [REF-CRY]).

2.4. Random number generator analysis

The random values necessary for the cryptographic mechanisms are generated by a random number generator available on the card.
The random number generator is a hardware generator associated with a software generator.

The hardware generator has not been analysed by the DCSSI.

The software generator consists of a random number software cryptographic post-treatment issued from the card hardware generator. The random number software cryptographic post-treatment mechanism reaches the “standard” level according to the French standard for cryptography (cf. [REF-CRY]). As stated in the document [REF-CRY], DCSSI reminds that for a cryptographic use, the hardware-generated numbers shall be reprocessed by a cryptographic algorithm, even if the analysed random number generator did not show any weakness.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for 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 products « eTravel EAC v1.1 80K (version 01 02) on P5CD080 » and « eTravel EAC v1.1 144K (version 01 02) on P5CD144 » submitted for evaluation fulfil the security features specified in the security target [ST] for the evaluation level EAL 4 augmented.

3.2. Restrictions

This certificate only applies on the products specified in chapter 1.2 of this certification report.

The user of the certified products shall respect the operational environmental security objectives specified in the security target [ST] chapter 4 and shall respect the recommendations given in the guidance [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:

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

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

Annexe 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	**2**	Problem tracking 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	**1**	Informal 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**	**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 Vulnerability assessment	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

Annexe 2. Evaluated products references

[ST]	Reference security target for the evaluation: - MAÏA EAC security target, Reference: ST_D1069147, version 0.7, Gemalto For the needs of publication, the following security target has been provided and validated in the evaluation: - MAÏA EAC Security target, Reference: ST_D1093538, version 1.0, Gemalto
[ETR]	Evaluation Technical Report – MAÏA project, Reference: MAÏA_ETR_v1.1, version 1.1, Serma Technologies
[ETR_ADD]	Evaluation Technical Report – Addendum – MAÏA project, Reference : MAÏA_ETR_ADD_v1.0, version 1.0, Serma Technologies
[2008_28]	Certification report DCSSI-2008/28 – « eTravel EAC version 1.1 sur composants P5CD080 et P5CD144 », 14th August 2008 SGDN/DCSSI
[CONF]	Class ACM : Configuration list, reference D1086734, version 0.5
[GUIDES]	Administration guidance: - MAÏA – Administrator guide, reference GUI_D1074871, version 1.2, Gemalto User guidance: - MAÏA – User guide, reference GUI_D1074872, version 1.1, Gemalto
[ANA-CRY]	Cotation de mécanismes cryptographiques – Projet MAÏA, N°2630/SGDN/DCSSI/SDS/DR du 20th November 2008 SGDN/DCSSI
[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, 19 November 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0026*

Annexe 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 the same as the international norm 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 the same as the international norm 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.
[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, N°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, BSI (Bundesamt für Sicherheit in der Informationstechnik)