PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/13

ID-One EPass 64 v2.0 with EAC RSA

Paris, 16th of May 2008

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.gouv.fr

Certification report reference

DCSSI-2008/13

Product name

ID-One EPass 64 v2.0 with EAC RSA

Product reference

Reference of the application: ePass 64k v2 (BAC AA EAC) v2.0 with patch « Optional Code r3.0 for ID One ePass 64K » v3.0

Reference of the microcontroller with embedded software: P5CD080UA/T0B16100

Protection profile conformity

BSI-PP-0026 rev: 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

Oberthur Technologies	NXP Semiconductors GmbH
71-73, Rue des Hautes Pâtures – 92726 Nanterre Cedex, France	Box 54 02 40, D-22502 Hamburg, Germany

Sponsor

Oberthur Technologies

71-73, Rue des Hautes Pâtures – 92726 Nanterre Cedex, France

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : 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 application "ID-One EPass 64 v2.0 with EAC RSA" developed by Oberthur Technologies, embedded on the P5CD080 V0B secure microcontroller developed and manufactured by NXP Semiconductors.

The evaluated product is a contactless smartcard with its antenna. It implements the travel document features according to the specifications from the International Civil Aviation Organization (cf. [ICAO]) and to the Extended Access Control (cf [EAC]). The contactless microcontroller with embedded software allows to check the authenticity of the travel document, and to identify its holder during a border control, with the support of an inspection system.. In particular, it enables:

- Protection in integrity of the holder's data stored: issuing state or organization, travel document number, expire date, holder's name, nationality, birth date, sex, holder's face portrait, other optional data, additional holder's biometric data and several other pieces of data for managing the document security;
- Authentication between the travel document holder and the inspection system prior to any border control by the Basic Access Control mechanism;
- Protection in integrity and confidentiality of data read by the secure messaging;
- Authentication of the genuine chip by the Active Authentication mechanism (if activated);
- Strong authentication of the chip and the inspection system prior to any biometric data retrieval.

The chip and its embedded software are intended to be inserted into the cover page of traditional passport booklets. They can be integrated into modules, inlay or datapage. The final product can be a passport, a plastic card etc…

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 conformant to the protection profile "Machine Readable Travel Document with ICAO Application, Extended Access Control" (cf. [PP EAC]).

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:

- Name and version of the product: ePass 64k v2 (BAC AA EAC) version 2.0;
- Name and version of the patch: Optional Code r3.0 for ID One ePass 64K version 3.0.

These elements can be identified with the command "Read Binary" applied on file "EF.TOE_Identification" as specified in the administration guidance (cf. [GUIDES]). The identifiers are:

- ROM Code Identifier: 067511;

- Patch code identified: 067843;
- PP identifier: 26 (for EAC);
- Product identifier: 03.

1.2.2. Security services

The product provides mainly the following security services:

- Access control in reading;
- Access control in writing;
- BAC mechanism;
- Secure messaging mechanism;
- Personalization agent authentication;
- Active authentication;
- EAC mechanism with RSA algorithm;
- Self tests;
- Safe state management;
- Physical protection;

The security services offered by the microcontroller are:

- Random number generator;
- Triple DES coprocessor;
- AES coprocessor;
- Control of operating conditions;
- Protection against physical manipulation;
- Logical protection;
- Protection of mode control;
- Memory access control;
- Special function register access control.

1.2.3. Architecture

The product consists of the microcontroller, the embedded operating system, the file system structure (LDS) and the commands for pre-personalization and personalization of the electronic travel document (Base card). The following picture sums up the product architecture:

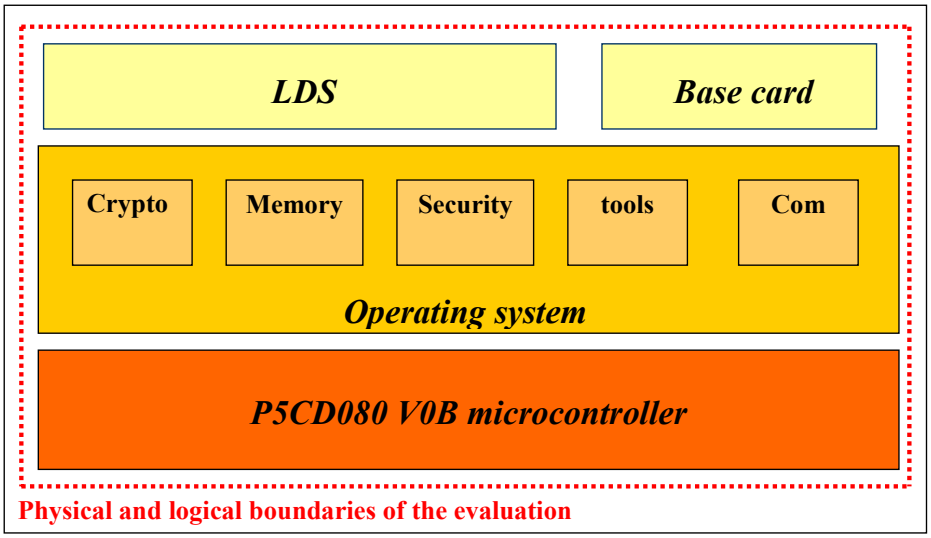

Figure 1 – Product architecture

1.2.4. Life cycle

The product's life cycle is organised as follow:

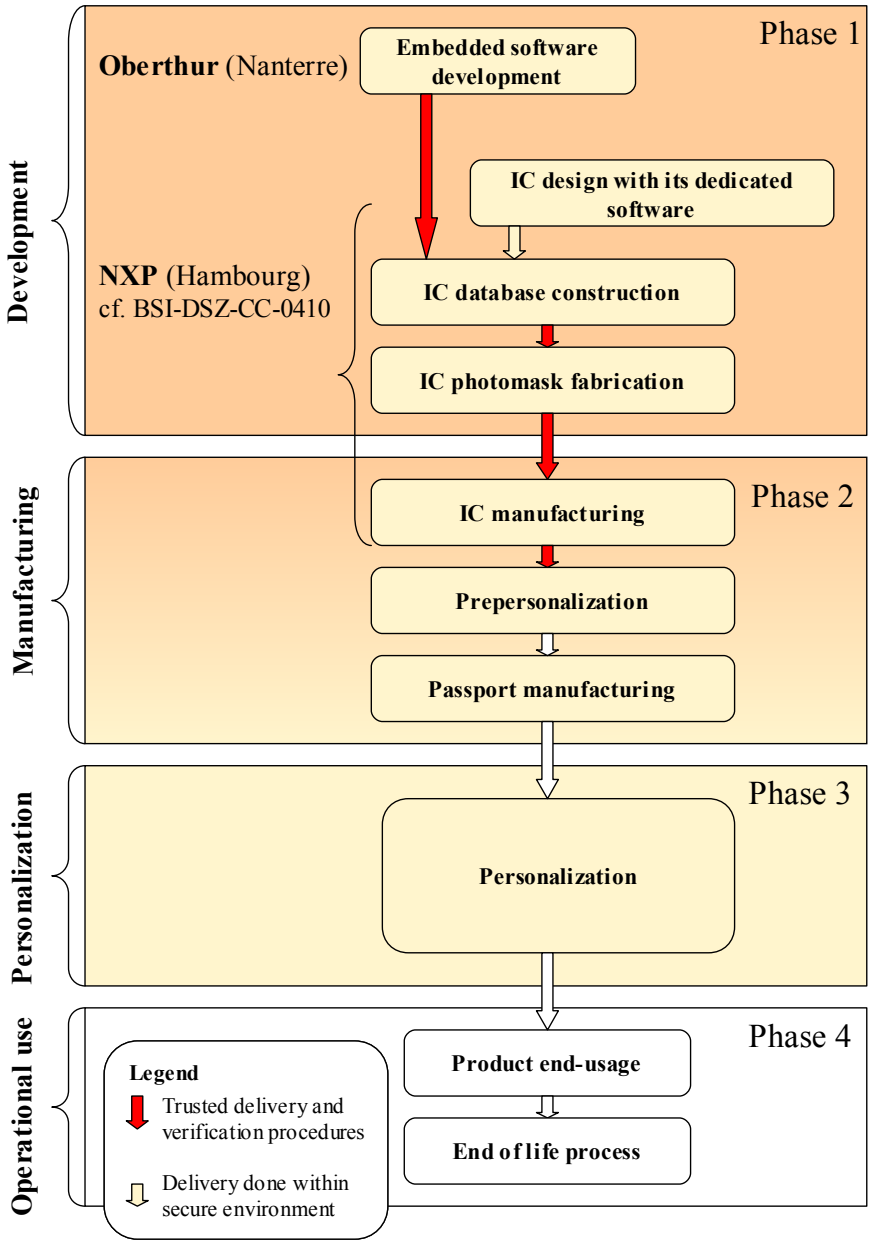

Figure 2 – Product Life-cycle

The product has been developed on the following sites:

Oberthur Technologies

71-73, Rue des Hautes Pâtures
92726 Nanterre Cedex,
France

The microcontroller is developed and manufactured by:

NXP Semiconductors

GmbHBox 54 02 40,
D-22502 Hamburg,
Germany

The manufacturing phase of the travel document (pre-personalization) can be performed either by Oberthur Technologies or by a subcontractor. This phase is not in the evaluation scope and is covered by guidance.

The travel document contains a patch built to bring functional modification of the product. This patch doesn't alter any security function or security countermeasure. Moreover, some mechanisms in the chip allow guarantying that the patch is developed by Oberthur Technologies and isn't modified. The patch can be loaded either by NXP in the IC manufacturing premises, or during the travel document manufacturing phase (pre-personalization) using the procedure described in the guidance (cf. [GUIDES]).

The phases of inlay and booklet manufacturing are not covered by the evaluation: it is considered that these phases have no impact on security, the product being self protected during these stages.

1.2.5. Evaluated configuration

The evaluated product is a 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 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 used evaluation methods consistent with [AIS 34] and validated by DCSSI.

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 evaluation of the microcontroller "P5CD080 V0B" 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 5th of July 2007 under the reference BSI-DSZ-CC-0410-2007.

The evaluation technical report [ETR], delivered to DCSSI the 10th of April 2008, 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 by DCSSI.

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 product "ID-One EPass 64 v2.0 with EAC RSA" 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 operational environmental security objectives summarized specified in chapter 4 of 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 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].

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

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, 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,

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:

Netherlands, New-Zealand, Norway, 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
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 of 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]	Reference security target for the evaluation: - Access World Security Target, Reference: 110 3851, édition : 1 Oberthur Technologies For the needs of publication, the following security target has been provided and validated in the evaluation: - ID-One™ ePass 64 v2.0 with EAC RSA – Security Target Lite, Reference: 110 4054 édition 1 Oberthur Technologies
[ETR]	Evaluation Technical Report - Access World project, Reference: AccessWorld_ETR_v1.0 version 1.0 Serma Technologies
[CONF]	Access World configuration list, Reference: 110 4048 édition 1-AA Oberthur Technologies
[GUIDES]	Access World Administration and User Guidance Document, Reference: FQR 110 3860 édition 1-AD Oberthur Technologies
[ICAO]	Doc 9303 Part 1 : Machine Readable Passports, volume 2 : Specifications for Electronically Enabled Passports with Biometric Identification Capability, reference: part 1, volume 2, Sixth Edition - 2006
[EAC]	Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v1.11
[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. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026*

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 - 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, 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