Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2015/62

ID-One ePass Full EAC v2 in PACE configuration on P60x080PVC/PVG components

Paris,

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 relating to this report should 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

certification@ssi.gouv.fr

Certification report reference

ANSSI-CC-2015/62

Product name

ID-One ePass Full EAC v2 in PACE configuration on P60x080PVC/PVG components

Product reference/version

SAAAAR 080031: ePass V3 Full EACv2 on NXP
SAAAAR 082455: Code r5.0 Generic
SAAAAR 082843: Optional Code r3.0 Digital Blurred Image

Protection profile conformity

BSI-CC-PP-0068-V2, [PP PACE], version 1.0
Machine Readable Travel Document using Standard Inspection Procedure with PACE

Evaluation criteria and version

Common Criteria version 3.1 revision 4

Evaluation level

EAL5 augmented
ALC_DVS.2, AVA_VAN.5

Developers

Oberthur Technologies
420 rue d'Estienne d'Orves
CS 40008
92705 Colombes, France

NXP Semiconductors
Box 54 02 40,
D-22502 Hamburg, Allemagne

Sponsor

Oberthur Technologies
420 rue d'Estienne d'Orves
CS 40008
92705 Colombes, France

Evaluation facility

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France

Applicable recognition agreements

CCRA

The product is recognised at EAL2.

SOG-IS

Introduction

Certification

Security certification for information technology products and systems is governed by decree number 2002-535 of 18th April 2002, modified. This decree stipulates that:

- The National Agency for Information Systems Security draws up **certification reports**. These reports indicate the features of the proposed security objectives. 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 (article 7).
- The **certificates** issued by the Prime Minister certify that 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 the regulations and standards in force, and with the required expertise 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 the "ID-One ePass Full EAC v2" smart card in PACE configuration on P60x080PVC/PVG components, and which can be used in contact and contactless mode. The product is developed by *Oberthur Technologies* on a component manufactured by *NXP Semiconductors*.

The product implements the travel document features in accordance with European specifications and those drawn up by the International and European Civil Aviation Organisation (ICAO). This product is used to verify the authenticity of the travel document and the identification of its holder during a border control, using an inspection system.

The evaluation target is composed of the ID-One ePass EAC application, in PACE (*Password Authenticated Connection Establishment*) configuration which carries out the electronic passport functions.

This micro-controller and its embedded software are intended to be inserted into the cover page of standard passports. They can be integrated into modules or *inlay*. The final product can be a passport, plastic card, etc.

1.2. Description of the product

1.2.1. Introduction

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

This security target is fully compliant with the protection profile [PP PACE].

1.2.2. Product identification

The constituent elements of the product are identified in the configuration list [CONF].

The certified version of the product can be identified by the following elements:

- commercial name: ID-One ePass Full EAC V2;
- code SAAAAR[1] of the ROM code: 080031;
- security patch code: C96E449AD06093BB25395B4F2C4F63720C46F52E2D4D91BA00B84B0986F7A738;
- optional patch code: B765E230D3B932A3930445DF453B50CAA3EC0077C03ABD2F327D8606532F51C2;
- component code (on 42 bytes): XXXXvvvvXX..XX where vvvv could be:
  - ‘6C14’ for component P60D080PVC;
  - ‘6014’ for component P60D080PVG;
  - ‘6019’ for component P60C080PVG.

[1] S: site code (0 for France), AAAA: article based on 4 numbers, R: software version or *release*.

It can be decided whether or not to load the optional *patch* and, thereby, whether or not to use the *Digital Blurred Image* function.

The "SAAAR and patch" codes can be verified using a GetData command with the DF66 tag. The component code can be verified using a GetData command with the 9F7F tag described in the [GUIDES].

1.2.3. Security services

The main security services provided by the product are:

- protection to ensure integrity of the card holder's data stored in the card: issuing nations or authorities, travel document number, expiry date, name of the holder, nationality, date of birth, sex, portrait, other optional data, additional biometric reference data and other data for managing the security of the travel document;
- controlling access to the card holder's data stored in the card;
- protection, to ensure integrity and confidentiality, of the data read using the *Secure Messaging* mechanism;
- validation of the chain of certificates;
- authentication of the micro-controller using the optional *"Active Authentication"* mechanism;
- authentication between the travel document and the inspection system during a border control by the PACE mechanism.

Digital Blurred Image is an optional function that has not been evaluated that makes the photo illegible in the case of fraudulent use.

1.2.4. Architecture

The product is a closed smart card comprised of the following components:

- a micro-controller P60x080PVC/PVG manufactured by *NXP Semiconductors*, in P60D080PVC, P60D080PVG or P60C080PVG configuration;
- "*BIOS*" software to access the micro-controller functionalities;
- a dedicated cryptographic library;
- a personalisation *"Perso"* application;
- an LDS[1] application supporting EAC, PACE and AA mechanisms.

[1] *Logical Data Structure*.

1.2.5. Life cycle

The product's life cycle is as follows:

	Phase	Actor	Covered by
Phase 1	Development	*OBERTHUR TECHNOLOGIES*	ALC
Phase 2	Development	*NXP SEMICONDUCTORS*	Component certification
Phase 3	Manufacturing	*NXP SEMICONDUCTORS*	Component certification
TOE delivery point			
Phase 4	MRTD manufacturer (Pre-perso)	MRTD manufacturer	AGD_PRE
Phase 5	MRTD manufacturer (Pre-perso)	MRTD manufacturer	AGD_PRE
Phase 6	Personalisation	Personalisation agent	AGD_PRE
Phase 7	Operational use	End user	AGD_OPE

The product was developed on the following site:

OBERTHUR TECHNOLOGIES **– Colombes site**
420 rue d’Estienne d’Orves
92700 Colombes
France

OBERTHUR TECHNOLOGIES **– Pessac site**
Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

The micro-controller is developed and manufactured by *NXP SEMICONDUCTORS*. The development and manufacturing sites for the micro-controller are detailed in the certification report with the reference [BSI-DSZ-CC-0837-V2-2014].

The "product administrators" are the issuing nations or authorities of the travel document.
The "product users" are the travellers and the inspection systems during the use phase.

1.2.6. Evaluated configuration

The product is a closed card that can be personalised under different configurations.
This certification report applies to the configuration including the following mechanisms:

- *Password Authenticated Connection Establishment*;
- *Active Authentication*.

The PACE mutual authentication mechanism between the card and the terminal was evaluated so as to be usable by any other application on the platform.

2. Evaluation

2.1. Evaluation reference bases

The evaluation was conducted in compliance with the **Common Criteria version 3.1 revision 4** [CC], using the evaluation methodology defined in the Common Evaluation Methodology [CEM] manual.

For assurance components that are not covered by the [CEM] manual, methods specific to the evaluation facility were used.

To meet the specifications of smart cards, the [JIWG IC] and [JIWG AP] guides were applied. Thus, the AVA_VAN level was determined using the rating scale of the [JIWG AP] guide. This rating scale is more demanding than that defined by default in the standard method [CC], used for other categories of products (software products for example).

2.2. Evaluation work

The composition evaluation was carried out according to the [COMP] guide to ensure that no weakness is introduced by the integration of the software in the micro-controller already certified.

Therefore, this evaluation took into account the results of the evaluation of the micro-controller "P60x080PVC/PVG" at level EAL6 augmented by the components ALC_FLR.1 and ASE_TSS.2, in accordance with the [BSI-PP-0035-2007] protection profile. This micro-controller was certified on 24th October 2014 under the reference [BSI-DSZ-CC-0837-V2-2014].

The evaluation technical report [ETR], submitted to ANSSI on 27th October 2015, details the work carried out by the evaluation facility and certifies that the status of all the evaluation tasks is "successful".

2.3. Cryptographic mechanisms rating according to the ANSSI's technical reference bases

The rating of the cryptographic mechanisms according to the ANSSI [REF] technical standard was not carried out. Nevertheless, the evaluation did not reveal any design and implementation vulnerabilities for the AVA_VAN.5 level targeted.

2.4. Random number generator analysis

The physical random number generator used by the final product was evaluated as part of the evaluation of the micro-controller (see [BSI-DSZ-CC-0837-V2-2014]).

In addition, as required in the ANSSI cryptographic standard ([REF]), the output of the physical random number generator undergoes reprocessing of a cryptographic nature.

The results were taken into account in the independent vulnerability analysis carried out by the evaluator and found no evidence of exploitable vulnerability for the AVA_VAN.5 level targeted.

3. Certification

3.1. Conclusion

The evaluation was carried out according to current rules and standards with the levels of competence and impartiality required for an approved evaluation centre. All of the evaluation work carried out enables a certificate to be issued according to decree 2002-535.

This certificate certifies that the product "ID-One ePass Full EAC v2" in PACE configuration on P60x080PVC/PVG components submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL5 augmented by components ALC_DVS.2 and AVA_VAN.5.

3.2. Restrictions

This certificate concerns the product specified in section 1 of this certification report.

The user of the certified product must ensure that the security objectives concerning the operating environment are complied with, as specified in the security target [ST], and follow the recommendations given in the guides provided [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 [SOGIS].

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. European recognition is applicable for smart cards and similar devices up to ITSEC E6 High and CC EAL7. The certificates that are recognised in the scope of the agreement are released with the following marking:

[1] The signatory countries of the SOG-IS agreement are: Austria, Finland, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and the 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 Agreement allows the recognition, by signatory countries[1], of the Common Criteria certificates.
Recognition is applicable up to the assurance components of CC EAL2 and also to ALC_FLR family.
The certificates that are recognised in the scope of the agreement 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, Pakistan, Spain, Sweden, Turkey, the United Kingdom and the United States.

Annexe 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level assigned to the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Name of the component
ADV **Development**	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD **User guides**	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	**5**	Development tools 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	**2**	Compliance with implementation standards
ASE **Evaluation of the security target**	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**	**3**	Testing: modular 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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Evaluated product references

[ST]	Reference security target for the evaluation: - MINOS – MRTD full EAC v2 Security Target PACE, version 7, reference: 110 7240, 21st October 2015, Oberthur Technologies. For the needs of publication, the following security target has been provided and validated in the evaluation: - Public Security Target PACE with AA, CA and PACE_CAM, version 4, reference: 110 7636, Oberthur Technologies.
[ETR]	Evaluation Technical Report: - Evaluation Technical Report – MINOS, version 1.2, reference LETI.CESTI.MIN.RTE.001, 27th October 2015, LETI.
[CONF]	Product configuration list: - MINOS ePass V3 Full EACv2 Configuration List, version 3, 23rd October 2015, reference 110 7577, Oberthur Technologies.
[GUIDES]	Product installation guide: - MINOS – MRTD FULL EAC V2 – Guidance Document – PREparative procedures, version 6, 8th October 2015, reference: 110 7111, Oberthur Technologies; - MINOS – MRTD FULL EAC V2 – Guidance Document – PREparative procedures PACE, version 3, 8th October 2015, reference: 110 7564, 15th June 2015, Oberthur Technologies. Product user guide: - MINOS – MRTD full EAC v2 – Guidance Document – OPErational user guidance, version 3, 24th June 2015, reference 110 7565, Oberthur Technologies.
[PP PACE]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0, 2nd November 2011. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0068-V2-2011*
[BSI-PP-0035-2007]	Security IC Platform Protection Profile, version 1.0, August 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*
[BSI-DSZ-CC-0837-V2-2014]	NXP Secure Smart Card Controller P60x080/052/040PVC(Y/Z/A)PVG with IC Dedicated Software. *Certified by BSI on 24 October 2014 under the reference BSI-DSZ-CC-0837-V2-2014.*

Annexe 3. References associated with certification

Decree number 2002-535 dated 18th April 2002, modified related to the security evaluation and certification for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 Certification of the security provided by information technology products and systems, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, September 2012, version 3.1, revision 4, reference CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, reference CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, reference CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September 2012, version 3.1, revision 4, reference CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smart cards, version 2.9, January 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2nd July 2014.
[SOG-IS]	"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, 8th January 2010, Management Committee.
[REF]	Cryptographic mechanisms – Rules and recommendations concerning the choice and sizing of cryptographic mechanisms, version 2.03 dated 21st February 2014, appended to the General Security Standard (RGS_B1), refer to www.ssi.gouv.fr.
	Cryptographic mechanisms – Rules and recommendations concerning the management of keys used in cryptographic mechanisms, version 2.00 dated 8th June 2012, appended to the General Security Standard (RGS_B2), refer to www.ssi.gouv.fr.

	Authentication – Rules and recommendations concerning the standard robustness level authentication mechanisms, version 1.0 dated 13th January 2010, appended to the General Security Standard (RGS_B3), refer to www.ssi.gouv.fr.

*SOG-IS document; in the scope of the CCRA recognition agreement, the equivalent CCRA supporting document applies.