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-2016/38

ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on P60x144PVA/PVE components

Paris, 23 june 2016

Courtesy Translation

SÉCURITÉ CERTIFICATION

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-2016/38

Product name

ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on P60x144PVA/PVE components

Product reference

SAAAAR 080031 : ePass V3 Full EACv2 on NXP

SAAAAR 082456 : Code r6.0 Generic

SAAAAR 082844 : Optional Code r4.0 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

EAL 5 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

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL2 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 the smart card « ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on P60x144PVA/PVE components », which can be in contact or contactless mode. This product is developed by *OBERTHUR TECHNOLOGIES* on a component manufactured by *NXP SEMICONDUCTORS*.

This product implements electronic travel document functionalities based on the International Civil Aviation Organization and the European Civil Aviation Conference specifications and requirements. This product is used to verify a travel document's authenticity and its holder identification during a border control process through an inspection system.

The evaluation target is composed of the ID-One ePass Full EAC v2 MRTD application, in PACE (*Password Authenticated Connection Establishment*) configuration with AA (*Active Authentication*), CA (*Chip Authentication*) and PACE CAM (*Password Authenticated Connection Establishment with Authentication Mapping)*, 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 *inlays*. The final product can be a passport, plastic card, etc.

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 fully compliant with the protection profile [PP PACE].

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 name: ID-One ePass Full EAC V2;
- SAAAAR[1] code of ROM code : 080031;
- Mandatory patch code : 412E4D1EC087005B56A9A2CAC0B6558F4CAAE041D8B5A69345559B562A6F4C8E;
- Optional patch code : E339C30BC6A81162413612FE2698284FA6CD28AA5CF5257A20B83611E58E9BEE;
- Component code (on 42 bytes): XXXXvvvvXX..XX where vvvv can take the following values:

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

- ‘6A15’ for P60D144PVA component;
- ‘6E15’ for P60D144PVE component;
- ‘6A20’ for P60C144PVA component;
- ‘6E20’ for P60C144PVE component.

It can be decided whether or not to load the optional patch and whether or not to the *Digital Blurred Image* function.
The "SAAAAR 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].

1.2.2. Security services

The main security services provided by the product are:

- Integrity Protection of the cardholder'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;
- Access control to the cardholder's data stored in the card;
- Integrity and confidentiality protection, through the *Secure Messaging* mechanism, of the data read on the card;
- Verification of the certificates’ validation chain;
- Authentication of the micro-controller using the optional « Active Authentication mechanisms »;
- Mutual authentication between the travel document and the inspection system by the PACE mechanism during border control process;
- Authentication of the travel document with the inspection system by the PACE mechanism in CAM mode.

There is an optional non evaluated function of *Digital Blurred Image* which makes the photo illegible in case of a fraudulent use.

1.2.3. Architecture

The product is a closed smart card which contained the following components:

- a micro-controller P60x144PVA/PVE manufactured by *NXP Semiconductors*, in P60D144PVA, P60D144PVE, P60C144PVA or P60C144PVE configuration;
- The "*BIOS*" software giving access to micro-controller functionalities;
- a dedicated cryptographic library;
- the *Perso* personalization application;
- a LDS[1] application supporting EAC, PACE, PACE CAM, CA and AA mechanisms;
- The eID application;
- The *eSign* application outside of the evaluation scope;
- The *Dauth* application outside of the evaluation scope.

[1] *Logical Data Structure*.

1.2.4. Life cycle

The product's life cycle is organised as follow:

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

The product has been 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 under the reference [BSI-DSZ-CC-0978-2016].
The "product administrators" are the nations or authorities issuing the driving license.
The "product users" are both the holders of driving license and the inspection systems during the use phase.

1.2.5. Evaluated configuration

The product is a closed card that can be personalized into 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 in order to be usable by any other application on the platform

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with the **Common Criteria version 3.1 revision 4** [CC], in accordance with the Common Evaluation Methodology defined in [CEM].

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

In order to meet specific features 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. For the record, 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 evaluation has been performed according to the composition scheme defined in the guide [COMP], in order to assess that no weakness arises from the integration of the software in the certified microcontroller.
Therefore, the results of the evaluation of the microcontroller « P60x144PVA/PVE » at EAL6 level augmented with ALC_FLR.1 and ASE_TSS.2 components, compliant with the [BSI-PP-0035-2007] protection profile, have been used. This microcontroller has been certified the 5th February 2016 under the reference [BSI-DSZ-CC-0978-2016].

The evaluation technical report [ETR], delivered to ANSSI the 18th March 2016, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis according to the ANSSI's technical standards

The rating of the cryptographic mechanisms robustness has been carried out according to the ANSSI [REF] technical standards.

The results obtained have been the subject of an analysis report [ANA-CRY] which leads to the following conclusions:

- The analyzed mechanisms are compliant to the ANSSI ([REF]) technical standard requirements, provided the recommendations mentioned in the guides (refer to [GUIDES]) are followed;
- The Hash function SHA-1 must not be used for signature applications.

As part of the reinforced qualification process, an expertise of cryptography's implementation was realized by the ITSEF. These results were taken into account in the independent vulnerability assessment realized by the evaluator and have not allowed to highlight exploitable vulnerabilities for the intended target namely AVA_VAN.5 level.

2.4. Random number generator analysis

The physical random number generator used by the final product was evaluated within the scope of the micro-controller evaluation (Refer to [BSI-DSZ-CC-0978-2016]).

In addition, as required in the ANSSI cryptographic standard ([REF]), the output of the physical random number generator is reprocessed using a cryptographic function.

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 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 « ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on P60x144PVA/PVE components » submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL5 augmented by ALC_DVS.2 and AVA_VAN.5 components.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1 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].

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

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[1], of the Common Criteria certificates. The recognition is applicable up to the assurance components of CC EAL2 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, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Component 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

Annex 2. Evaluated product references

[ST]	Reference Security target for the evaluation: - MINOS – ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE – Security Target, version 2, reference : 110 7888, 2nd March 2016, Oberthur Technologies. For publication needs, the following security target has been provided and validated for the present evaluation : - ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE – Public Security Target, version 2, reference: 110 7965, Oberthur Technologies.
[ETR]	Evaluation Technical Report : - Evaluation Technical Report – MINOS MRTD, version 2.0, reference LETI.CESTI.MIN.RTE.001, 18th March 2016, LETI.
[ANA-CRY]	MINOS – Cryptographic sizing mechanism MRTD, version 2.0, reference: LETI.CESTI.MIN.RT.033, 18th March 2016, LETI.
[CONF]	Product configuration list: - MINOS ID-One ePass Full EACv2 MRTD and ID-One eIDL Configuration List, version 2, 16th March 2016, reference 110 7903, Oberthur Technologies.
[GUIDES]	Product installation guide : - MINOS – MRTD FULL EAC V2 – Guidance Document – PREparative procedures, version 11, 2nd March 2016, reference : 110 7111, Oberthur Technologies ; - MINOS – ID-One ePass Full EACv2 MRTD in PACE configuration with AA, CA and PACE CAM – Guidance Document – PREparative procedures, version 2, reference : 110 7929, 16th March 2016, 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-0978-2016]	NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software. *Certified by BSI on February 5th 2016 under the reference BSI-DSZ-CC-0978-2016.*

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 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 smartcards, 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 regarding 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 keys management – 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.