PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report 2007/06

Oberthur Card ID-One ePass 64K: application ID-One ePass 64K v1.0 masked on Philips (NXP) components P5CD072/V0P and P5CD072/V0Q

Paris, 23rd March 2007

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.pm.gouv.fr

Reproduction of this document without any change or cut is authorised.

Certification report reference

2007/06

Product name

Oberthur Card ID-One ePass 64K: application ID-One ePass 64K v1.0 masked on Philips (NXP) components P5CD072/V0P and P5CD072/V0Q

Product reference

Philips references IC + ROM mask : 9352 831 41006 VOP et 9352 831 64118 VOQ

Protection profile conformity

« Machine readable Travel Document with ICAO Application, Basic Access Control » BSI-PP-0017 rev: 1.0 date 18/08/2005

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

Developer(s)

Oberthur Card Systems SA
71-73 rue des Hautes Pâtures
92726 Nanterre, France

Philips Semiconductors
Postfach 54 02 40,
D-22502 Hamburg, Allemagne

Sponsor

Oberthur Card Systems SA
71-73 rue des Hautes Pâtures, 92726 Nanterre, France

Evaluation facility

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

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 « Oberthur Card ID-One ePass 64K: application ID-One ePass 64K v1.0 masked on Philips (NXP) components P5CD072/V0P and P5CD072/V0Q » is an electronic passport developed by Oberthur Card Systems SA.

The assessed product is a contactless smartcard with antenna. It implements the electronic passport functionalities as per the specifications of the international Civil Aviation Organization (see [ICAO]). The product itself is a contactless interface controller with an onboard software application enabling the following:

- To store signed data items for the future passport holder (issuing organization or country, passport number, expiry date, name of holder, nationality, date of birth, sex, any other optional information); a biometric data item regarding the holder (photo of face); optional authentication data and other miscellaneous data used to handle document security;
- To check the authenticity of passport and identify its holder when going through customs, by means of an inspection system. This microcircuit and its onboard software application are designed to be inserted in the cover of standard passports.

1.2. Evaluated product description

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

This security target is compliant to “Machine readable Travel Document with ICAO Application, Basic Access Control” protection profile [PP MRTD].

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:

- ROM: EV4/T0QE1040
- TOE name: ID One ePass 64K
- TOE version : 1.0
- Microcontroller: Philips Smart MX P5CD072 V0Q and VOP
- Customer ROM code Identification : LDS 1.7 72K V1.0 RC
- TOE reference IC + ROM mask:
  12NC: 9352 831 41006 VOP et 12NC: - 9352 831 64 118 VOQ

1.2.2. Security services

The main security services provided by the product are:

- Access control on the product lifecycle phases;
- Authentication mechanisms ("Basic Access Control" and "Active Authentication");
- Data exchange with "Secure Messaging".

1.2.3. Architecture

The product consists of the following:

- a controller with a contactless interface and a dedicated software;
- dedicated test software and support software;
- embedded software (operating system);
- MRTD application.

1.2.4. Life cycle

The product's life cycle is organised as follow:

Phase 1	IC design	The IC design is done by NXP. IC Dedicated Software and the guidance documentation are done by NXP.
	E-passport embedded software development	The software developer is Oberthur Card Systems.
	Code Delivery	The Rom Code and EEPROM initialization data are delivered by OCS to NXP
Phase 2	IC Manufacturing	The IC manufacturing is performed on behalf of NXP
	IC Pre Personalization	The IC manufacturer is responsible for the pre-personalization of the TOE.
	IC Testing	The Ic manufacturer performs testing of the TOE
	IC and guidance delivery	The IC is provided by NXP and the guidance is provided to the personalizer by OCS
Phase 3	E-passport printing	The personalizer prints the e-passport and embeds the contactless IC with its antenna in the booklet
	E-passport Personalization	The personalizer is responsible for the E-passport personalization .
	E-passport testing and packaging	The personalizer is responsible for testing and packaging.
Phase 4	E-passport use phase	The E-passport issuer is responsible for the e-passport product delivery to the e-passport holder.

The product has been developed on the following site:

Oberthur Card Systems

71/73 rue des Hautes Pâtures
92726 Nanterre
France

Neither the inlay phase nor the integration of the inlay into the passport itself is included in the evaluation. However, this will have no impact on the level of security since the product is protected during these phases.

1.2.5. Evaluated configuration

The certificate applies to the following configurations detailed in the guides [GUIDES]:

- Controller configured with the options "card disable feature" at 'enabled'; "ROM read from EEPROM feature" at 'disabled' and "Ram execution feature" at 'disabled';
- Application configured with the options: "BAC" at enabled, "test mode" at disabled, "debrayed mode" at disabled, "erase card" at disabled and "Random UID" at enabled.

No softmask is loaded, neither by the developer nor at any subsequent stage.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC], with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CCAP] guide has 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 "*Philips Secure Smart Card Controller P5CD072V0P"* and "*Philips Secure Smart Card Controller P5CD072V0Q"* both of them evaluated at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 compliant with the [PP0002] protection profile. These microcontrollers have been certified the 28th March 2006 under the reference BSI_DSZ_CC_0348_2006 and BSI_DSZ_CC_0349_2006.

The evaluation technical report [ETR], delivered to DCSSI the 20th February 2007, 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 been analysed by DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY] and have been taken into account in the evaluator vulnerability analysis.

3. Certification

3.1. Conclusion

The evaluation identified in chapter 2 and described in the evaluation technical report [ETR], was carried out according to the current rules and standards, with the required competency and impartiality by 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 "Oberthur Card ID-One ePass 64K: application ID-One ePass 64K v1.0 masked on Philips (NXP) components P5CD072/V0P and P5CD072/V0Q" 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 specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organization:
  - Establish the correct identity of the holder and create biographic data for the MRTD;
  - Enrol the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s);
  - Personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the Document Security Object). The Personalization Agents enable or disable the Basic Access Control function of the TOE according to the decision of the issuing State or Organization. If the Basic Access Control function is enabled the Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip;
- The Issuing State or Organization must:
  - Generate a cryptographic secure Country Signing Key Pair;
  - Ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment;
  - Distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity;

  The Issuing State or organization must:
  - Generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys;
  - Sign Document Security Objects of genuine MRTD in a secure operational environment only;

  - Distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object includes all data in the data groups DG1 to DG16 if stored in the LDS according to [ICAO];
- The issuing State or Organization has to establish the necessary public key infrastructure in order to:
  - Generate the MRTD's Active Authentication Key Pair,
  - Sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15,
  - Support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object;
- The issuing State or Organization must ensure that the MRTD administrator acting on the behalf of the issuing State or Organization establish the correct identity of the holder and update the MRTD with the defined physical and logical security measures. According to the decision of the issuing State or Organization the MRTD administrator can for example terminate the application or execute any administrative commands provided by the TOE;
- The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. Additionally the Extended Inspection System performs the Active Authentication mechanism to verify the Authenticity of the presented MRTD's chip;
- The border control officer of the Receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems;
- The inspection system of the receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems, which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system;
- The holder may prevent attempts to disclose the logical MRTD by following recommendations for the protection of the MRZ against unauthorized people. An attacker knowing the MRZ or a part of it have better chance to perform a successful skimming or eavesdropping attack.

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 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, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland 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 Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, United Kingdom and United States.

Annex 1. Evaluation level of the product

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ACM Gestion de configuration	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 Livraison et opération	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 Développement	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 Guides d'utilisation	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 Support au cycle de vie	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 Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - "E-PASSPORT Security Target" ref : FQR 110 3435 rev : 1-AF date : February 19th 2007 For the needs of publication, the following security target has been provided and validated in the evaluation: - E-passport 72K - Public Security Target ref: 110 3674 V1.0
[ETR]	Evaluation technical report : - Evaluation Technical Report, ref. LETI.CESTI.BIS.RTE.001 – v2.0, date : February 19th 2007 - Evaluation Technical Report Addendum ref. LETI.CESTI.BIS.RTE.002 - v1.0 – date : March 9th 2007
[ANA-CRY]	Cotation de mécanismes cryptographiques - Projet BISON n° 45/SGDN/DCSSI/SDS/Crypto
[CONF]	BISON Configuration List FQR 110 3510 v1.0 – date : March 7th 2007
[GUIDES]	Administration and user guidance: - Application LDS V1.7 72K on P5CD072 SOFTWARE REQUIREMENT SPECIFICATION (SRS) ref. FQR : 110 3484 rev.2-AB - BISON Administration Guidance ref. FQR : 110 3484 rev.1-AB, date : February 1st 2007
[OACI]	- PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004 International Civil Aviation Organization, - Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004, International Civil Aviation Organization, Machine Readable Travel Documents supplement 9303
[PP MRTD]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, August 18th 2005. Certifié sous la référence BSI-PP-0017
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié sous la référence BSI-PP-0002-2001.*

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 AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, Version 1.10, 19th December 2006, ref: 2791/SGDN/DCSSI/SDS/Crypto.