Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2007/06

Carte Oberthur ID-One ePass 64K : application ID-One ePass 64K v1.0 masquée sur les composants Philips (NXP) P5CD072/V0P et P5CD072/V0Q

Paris, le 23 mars 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

2007/06

Nom du produit

Carte Oberthur ID-One ePass 64K : application ID-One ePass 64K v1.0 masquée sur les composants Philips (NXP) P5CD072/V0P et P5CD072/V0Q

Référence/version du produit

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

Conformité à un profil de protection

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

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2

Développeur(s)

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

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

Commanditaire

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

Centre d'évaluation

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

Accords de reconnaissance applicables

CCRA

SOG-IS

IT Security Certified

Le produit est reconnu au niveau EAL4

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué : « Carte Oberthur ID-One ePass 64K : application ID-One ePass 64K v1.0 masquée sur les composants Philips (NXP) P5CD072/V0P et P5CD072/V0Q » est un passeport électronique développé par Oberthur Card Systems SA.

Le produit évalué est de type carte à puce sans contact avec antenne. Il implémente les fonctionnalités de passeport électronique conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale (cf. [OACI]). Il s'agit d'un microcontrôleur à interface sans contact avec un logiciel embarqué permettant :

- de stocker les données signées du futur porteur du passeport (nation ou organisation émettrice, n° de passeport, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, données d'informations optionnelles), une donnée biométrique du porteur (photo du visage), des données d'authentification optionnelles et diverses données permettant de gérer la sécurité du document ;
- de vérifier l'authenticité du passeport et d'identifier son porteur lors d'un contrôle frontalier à l'aide d'un système d'inspection. Ce microcircuit et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection « Machine Readable Travel Document with ICAO Application, Basic Access Control » [PP MRTD].

La cible de sécurité ajoute par rapport au profil de protection l'« Active Authentication » dans le périmètre de l'évaluation.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

- 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. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- contrôle d'accès sur les différentes phases du cycle de vie ;
- mécanismes d'authentification (« Basic Acces Control » et « Active authentication ») ;
- échanges de données par « Secure Messaging ».

1.2.3. Architecture

Le produit est constitué :

- d'un microcontrôleur avec une interface sans contact et son logiciel dédié,
- d'éléments logiciels de test et de support dédiés,
- d'un logiciel embarqué (système d'exploitation),
- et de l'application MRTD.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

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.

Le produit a été développé sur le site suivant :

Oberthur Card Systems

71/73 rue des Hautes Pâtures
92726 Nanterre
France

Les phases de mise en « inlay » et d'intégration de « l'inlay » dans le livret du passeport ne sont pas couvertes par l'évaluation, mais n'ont de toute façon pas d'impact sécuritaire, le produit étant protégé durant ces phases.

1.2.5. Configuration évaluée

Le certificat porte sur les configurations suivantes, détaillées dans les guides [GUIDES] :

- microcontrôleur configuré avec les options « card disable feature » activée, « rom read from EEPROM feature » désactivée et « Ram execution feature » désactivée ;
- application configurée avec les options : « BAC » activée, « test mode » désactivée, « debrayed mode » désactivée, « erase card » désactivée et « Random UID » activée.

Aucun Correctif (softmask) n'est chargé, ni chez le fondeur ni après.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, le guide [CCAP] a été appliqué.

2.2. Travaux d'évaluation

L'évaluation a été réalisée en composition en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans les microcontrôleurs déjà certifiés par ailleurs.
Cette évaluation a ainsi pris en compte les résultats des évaluations des microcontrôleurs « *Philips Secure Smart Card Controller P5CD072V0P* » et « *Philips Secure Smart Card Controller P5CD072V0Q* », *tous deux évalués* au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, et conforme au profil de protection [PP0002]. Ces microcontrôleurs ont été certifiés le 28 mars 2006 sous les références BSI_DSZ_CC_0348_2006 et BSI_DSZ_CC_0349_2006.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 20 février 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Carte Oberthur ID-One ePass 64K : application ID-One ePass 64K v1.0 masquée sur les composants Philips (NXP) P5CD072/V0P et P5CD072/V0Q» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- l'Etat émetteur ou l'organisation doit s'assurer que les utilisateurs agissant en tant qu'agents de personnalisation :
  - établissent l'identité correcte du porteur du passeport et identifient ses données biographiques pour le passeport électronique ;
  - enregistrent les données biométriques de référence du porteur, c'est-à-dire son portrait ;
  - personnalisent le passeport pour le porteur avec les mesures sécuritaires physiques et logiques requises (incluant la signature électronique des données du porteur dans le passeport). L'agent de personnalisation active la fonction de contrôle d'accès basique (BAC) et génère la clé de contrôle d'accès basique dans le passeport. L'agent de personnalisation doit générer des clés cryptographiques de 112 bits conformément à l'algorithme de dérivation des clés BAC spécifié dans l'annexe E du document [OACI] relatif à la PKI ;
- l'Etat émetteur ou l'organisation doit :
  - générer une bi-clé de signature nationale cryptographiquement sûre ;
  - garantir le secret de la clé privée de cette bi-clé nationale de signature et signer les certificats des signataires de document dans un environnement opérationnel sécurisé ;
  - distribuer un certificat de la clé publique nationale de signature aux Etats et organisations. Ce certificat assure l'intégrité et l'authenticité de cette clé.

  L'Etat émetteur ou l'organisation doit également :
  - générer une bi-clé de signature des documents cryptographiquement sûre ;

  - garantir le secret de la clé privée de cette bi-clé de signature de document, et signer les données sécuritaires d'un passeport authentique dans un environnement opérationnel sécurisé ;
  - distribuer aux Etats et organisations le certificat de la clé publique de signature de document signé avec la clé publique nationale, en maintenant son intégrité et son authenticité en utilisant l'infrastructure de clés décrite dans [OACI] ;
- l'Etat émetteur ou l'organisation doit :
  - générer une bi-clé d'authentification active du passeport ;
  - signer et stocker dans le passeport la clé publique d'authentification active ;
  - fournir un support aux systèmes d'inspection des Etats et organisations, pour vérifier l'authenticité des passeports électroniques en certifiant la clé publique d'Authentification Active (AA) ;
- l'Etat ou l'organisation émetteur doit garantir que les administrateurs agissant pour leur compte établissent correctement l'identité du porteur et mettent à jour les passeports avec les mesures physiques et logiques requises. Selon la décision de l'Etat ou l'organisation émetteur, l'administrateur peut par exemple désactiver l'application ou exécuter les commandes d'administration proposées par le produit ;
- le système d'inspection de l'Etat ou l'organisation doit vérifier le passeport présenté par le voyageur pour vérifier son authenticité à l'aide de moyens physiques, et pour détecter toute manipulation physique du passeport. Le système d'inspection étendu utilise le mécanisme « Active authentication » pour vérifier l'authenticité de la puce du passeport présenté ;
- le système d'inspection doit vérifier la signature des données signées du passeport préalablement à leur utilisation pour identifier le porteur. Les Etats et organisations doivent maintenir l'authenticité et la disponibilité des clés publiques de signature nationales et de signature des documents au sein de tous les systèmes d'inspection ;
- le système d'inspection des Etats et des organisations doit garantir la confidentialité et l'intégrité des données lues dans le passeport. Les Etats et organisations examinant le passeport en mettant en œuvre le protocole BAC doivent utiliser un terminal d'inspection implémentant la partie « terminal » du protocole BAC afin de chiffrer les communications et données transmises entre le passeport et le terminal. Les Etats et organisations utilisant le mode primaire (Primary inspection system) mettront en œuvre des mesures empêchant l'écoute passive des communications entre le terminal et le passeport ;
- le porteur ne doit pas divulguer les données de son passeport à des tiers non autorisés. Un attaquant connaissant la bande MRZ (données imprimées sur le passeport utilisées pour dériver la clé d'accès aux données stockées dans la puce) ou une partie de ces données aura plus de chance de réaliser une attaque par écoute passive ou par tentative de communication avec le passeport à l'insu de son porteur.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[2] Les pays signataires de l'accord sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle-Zélande, la Norvège, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

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

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - "E-PASSPORT Security Target" ref : FQR 110 3435 rev : 1-AF date : 19/02/07 Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - E-passport 72K - Public Security Target ref: 110 3674 V1.0
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report, ref. LETI.CESTI.BIS.RTE.001 – v2.0 du 19/02/07 - Evaluation Technical Report Addendum ref. LETI.CESTI.BIS.RTE.002 - v1.0 – du 09/03/07
[ANA-CRY]	Cotation de mécanismes cryptographiques - Projet BISON n° 45/SGDN/DCSSI/SDS/Crypto
[CONF]	BISON Configuration List FQR 110 3510 v1.0 - du 07/03/07
[GUIDES]	Guides d'administration et d'utilisation du produit : - 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, 01/02/07
[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, 18 August 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.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, 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. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale 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 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/LCR.