



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

Rapport de certification ANSSI-CC-2014/01

**ePass V3 TD sur composants P5CD081V1A, en
configuration EAC sur SAC via PACE v2 et AA**

Paris, le 28 janvier 2014

*Le directeur général de l'agence nationale
de la sécurité des systèmes d'information*

Patrick Pailloux
[ORIGINAL SIGNE]



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 présumées 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), 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 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.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2014/01

Nom du produit

ePass V3 TD sur composants P5CD081V1A, en configuration EAC sur SAC via PACE v2 et AA

Référence/version du produit

SAAAAR ROM 079161, SAAAAR Codop 079223

Conformité à un profil de protection

**Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE,
Version 1.3.2, BSI-CC-PP-0056-V2-2012**

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

**EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5**

Développeurs

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

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

Commanditaire

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

Centre d'évaluation

Serma Technologies
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables



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 modifié. Ce décret indique que :

- L'agence nationale 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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	7
1.2.4. <i>Architecture</i>	7
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	9
3. LA CERTIFICATION	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS D’USAGE.....	10
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	12
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	13
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	14

1. Le produit

1.1. Présentation du produit

Le produit évalué est le passeport électronique « ePass V3 TD sur composants P5CD081V1A, en configuration EAC sur SAC via PACE v2 et AA », référence SAAAAR ROM 079161, SAAAAR Codop 079223, développé par Oberthur Technologies sur un composant NXP Semiconductors.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (OACI¹). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module ou d'*inlay*. Le produit final peut être un passeport, une carte plastique, etc.

1.2. Description du produit

1.2.1. Introduction

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 [PP0056V2]. Il s'agit d'une conformité stricte. Le profil de protection [PP0056V2] est strictement conforme au profil de protection [PP0068V2]. La cible de sécurité est donc également strictement conforme à [PP0068V2].

1.2.2. 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 :

- nom commercial : ePass V3 TD ;
- code SAAAAR² du code ROM : 079161 ;
- code SAAAAR du code optionnel (*patch*) : 079223.

Ces codes peuvent être vérifiés par une commande GETDATA avec le tag DF52 comme décrit dans [GUIDES].

¹ Encore appelé ICAO pour *International Civil Aviation Organization*.

² S désignant le code site (0 pour la France), AAAA: article sur 4 digits, R : release ou version du logiciel.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

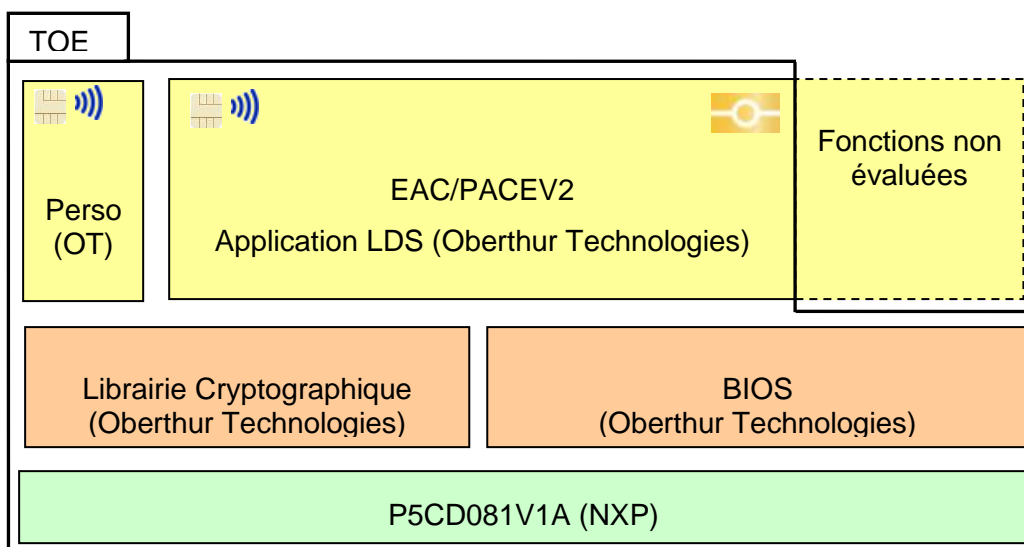
- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme SAC (« *Supplemental Access Control* ») ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues ;
- l'authentification du microcontrôleur par le mécanisme optionnel « *Active Authentication* ».

1.2.4. Architecture

Le produit est une carte à puce fermée constituée des éléments suivants :

- un microcontrôleur P5CD081V1A de NXP Semiconductors, en configuration P5CD081V1A, P5CC081V1A ou P5CD041V1A ;
- un logiciel « *BIOS* » donnant l'accès aux fonctionnalités du microcontrôleur ;
- une librairie cryptographique dédiée ;
- une application de personnalisation « *Perso* » ;
- l'application LDS¹ supportant les mécanismes EAC, PACEV2 et AA.

La figure suivante représente cette architecture :



1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 2.3 de la cible de sécurité [ST].

Les sites de développement et de production du microcontrôleur sont identifiés dans les rapports de certification [CERT_IC].

¹ Logical Data Structure.

Les sites audités dans le cadre de cette évaluation sont les sites de développement du logiciel embarqué suivants :

Oberthur Technologies – Site de Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Site de Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies – Site de Pessac

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

Oberthur Technologies – Site de Colombes

420 rue d'Estienne d'Orves
92700 Colombes
France

1.2.6. Configuration évaluée

Le produit est une carte fermée qui peut être personnalisée selon différentes configurations.

Le certificat porte sur la configuration suivante :

- mécanisme SAC (PACE V2) activé ;
- mécanisme *active authentication* activé (ECC ou RSA).

Le mécanisme de chargement de correctif (*patch*) a été évalué.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4 [CC]** et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « P5CD081V1A » au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été re-certifié le 12 juin 2013, voir [CERT_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 décembre 2013, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur physique du microcontrôleur a été évalué dans le cadre de l'évaluation [CERT_IC]. Le générateur d'aléas utilisé par la carte s'appuie sur le générateur physique fourni par le microcontrôleur associé à un retraitement. L'évaluation n'a pas mis en évidence de vulnérabilités pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour 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 « ePass V3 TD sur composants P5CD081V1A, en configuration EAC sur SAC via PACE v2 et AA », référence SAAAAR ROM 079161, SAAAAR Codop 079223, soumis à l'évaluation, répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

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 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé 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 CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

² Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, 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 5+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation : TARANIS Security Target EAC on SAC, FQR 110 6358 Ed 5, 16 octobre 2013, Oberthur Technologies.</p> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : ePASS V3 TD TARANIS, EAC on SAC passport, Public Security Target, FQR 110 6667 Ed 1, Oberthur Technologies.</p>
[RTE]	<p>Evaluation Technical Report – TARANIS Project, TARANIS_ETR_v2.0/2.0, 4 décembre 2013, Serma Technologies.</p>
[CONF]	<p>TARANIS Configuration list, FQR 110 6612 Ed 3, 6 décembre 2013, Oberthur Technologies.</p>
[GUIDES]	<ul style="list-style-type: none"> - TARANIS Guidance, FQR 110 6468 Ed 2, 23 avril 2013, Oberthur Technologies ; - TARANIS Administration and Personalization Guidance document, FQR 110 6450 Ed 5, 7 octobre 2013, Oberthur Technologies.
[PP0056V2]	<p>Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012.</i></p>
[PP0068V2]	<p>Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011.</i></p>
[PP0035]	<p>Security IC Platform Protection Profile, Version 1.0. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i></p>
[CERT_IC]	<ul style="list-style-type: none"> - Rapport de certification BSI-DSZ-CC-0555-2009 pour le produit “NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software”, 10 novembre 2009 ; - Rapport de certification BSI-DSZ-CC-0857-2013 pour le produit “NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081 V1A/V1A(s)”, 12 juin 2013.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, March 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, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.</p> <p>Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr.</p>

Authentification – Règles et recommandations concernant les mécanismes d’authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_3), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l’accord de reconnaissance du CCRA, le document support du CCRA équivalent s’applique.