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-2011/21

Passeport electronique EAC PEACOS sur P5CD080 V0B, version 1.2

Paris, le 1er juillet 2011

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

Patrick Pailloux
[ORIGNAL 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 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 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

Référence du rapport de certification

ANSSI-CC-2011/21

Nom du produit

Passeport electronique EAC PEACOS sur P5CD080 V0B

Référence/version du produit

PEACOS_NXP80_1_2 / Version 1.2

Conformité à un profil de protection

[PP EAC], version 1.2

Machine Readable Travel Document with "ICAO Application", Extended Access Control

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Gep S.p.A

90 Corso Salvatore D'Amato, 80022 Arzano, Italy

NXP Semiconductors Germany GmbH

Box 54 02 40, D-22502 Hamburg, Germany

Commanditaire

Istituto Poligrafico e Zecca dello Stato S.p.A

1027 Via Salaria , 00198 Roma, Italy

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

Accords de reconnaissance applicables

CCRA

SOG-IS

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

1.1. Présentation du produit

Le produit évalué est « Passeport electronique EAC PEACOS sur P5CD080 V0B, référence PEACOS_NXP80_1_2 / Version 1.2 » développé par Gep S.p.A et NXP Semiconductors.

Le produit évalué est de type carte à puce sans contact. Il implémente les fonctionnalités de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale. Ce produit est destiné à vérifier l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

1.2. Description du produit

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 [PP EAC]. Il s'agit d'une conformité démontrable.

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 à partir des éléments suivants :
- référence commerciale du produit (Gep S.p.A) : PEACOS Electronic Passport, version 1.2 ;
- nom et version du microcontrôleur (NXP): P5CD080 V0B ;
- référence complète du logiciel embarqué (Gep S.p.A): PEACOS_NXP80_1_2 ;
- référence fondeur (NXP) : P5CD080A4/T0B26350 (puce masquée), PEACOS_FK03.hex (patch).

La version du produit peut être vérifiée à l'aide de sa réponse à la commande « Get Data » avec P1 = 01h et P2 = 10h :

50h 45h 41h 43h 4Fh 53h 5Fh 4Eh 58h 50h 38h 30h 5Fh 31h 5Fh 32h.

Cette réponse est interprétée comme suit :
- identifiant de l'OS : 50h 45h 41h 43h 4Fh 53h 5Fh (PEACOS_) ;
- identifiant du microcontrôleur : 4Eh 58h 50h 38h 30h 5Fh (NXP80_) ;
- version de l'OS : 31h 5Fh (1_) ;
- version du patch : 32h (2).

1.2.2. Services de sécurité

Les principaux services de sécurité évalués fournis par la TOE sont :

- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, données biométriques additionnelles, données permettant de gérer la sécurité du document de voyage et autres données optionnelles ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme BAC (*Basic Access Control*) ;
- la protection de l'intégrité et de la confidentialité des données lues à l'aide du mécanisme S*ecure Messaging* ;
- l'authentification forte entre le microcontrôleur et le système d'inspection par le mécanisme EAC (*Extended Access Control*) préalablement à tout accès aux données biométriques.

1.2.3. Architecture

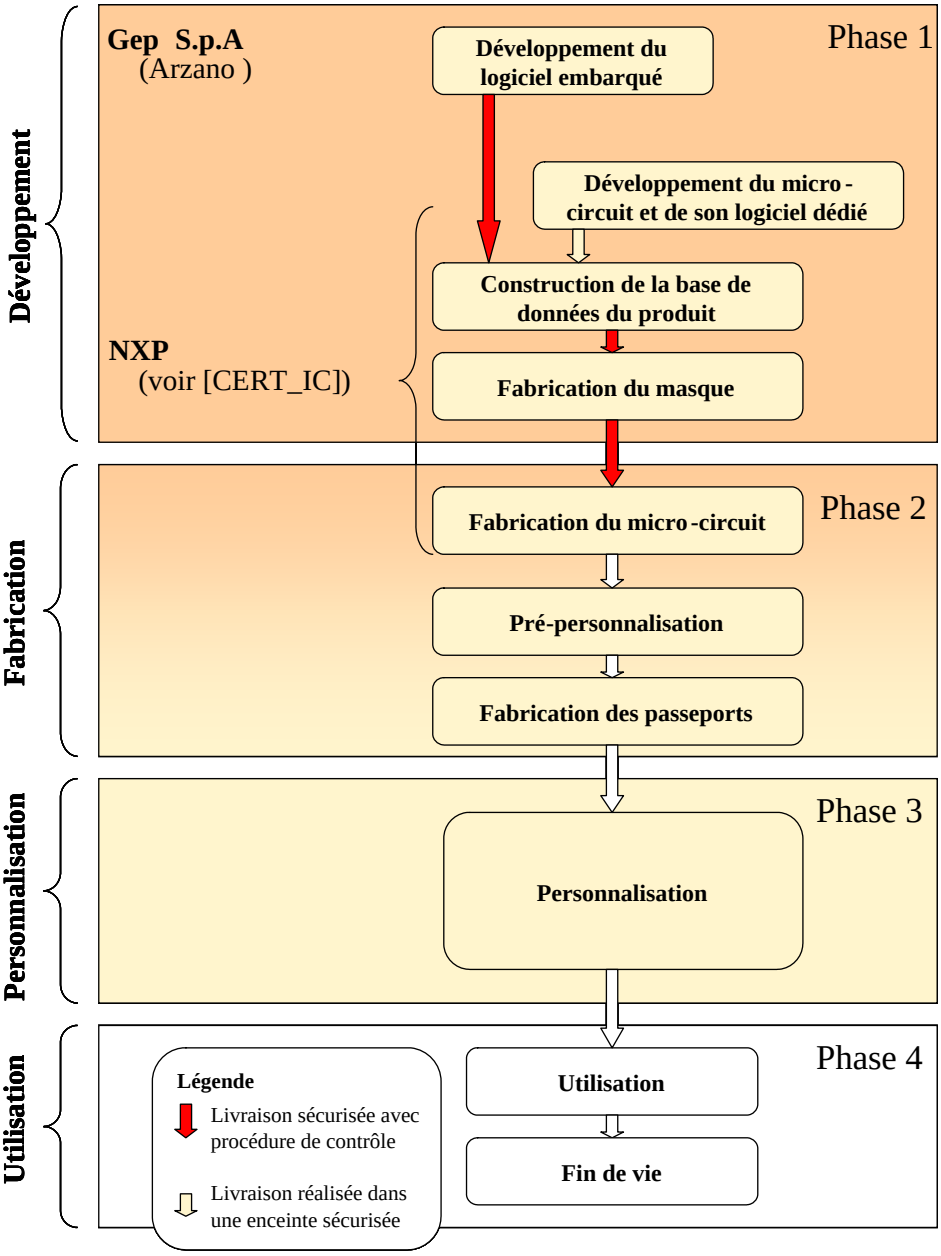
Le produit est constitué :

- du microcontrôleur P5CD080 V0B, développé et fabriqué par NXP ;
- du logiciel dédié au microcontrôleur, développé par NXP ;
- des parties logicielles, développées par Gep S.p.A, de référence PEACOS_NXP80_1_1, masquées dans la ROM du microcontrôleur, composées :
    - du système d'exploitation, qui inclut la couche d'abstraction du matériel HAL[1] ;
    - et de l'application MTRD ;
- du patch logiciel, développé par Gep S.p.A, de référence PEACOS_FK03, chargé dans l'EEPROM du microcontrôleur.

[1] Hardware Abstraction Layer

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le logiciel embarqué du produit a été développé sur le site suivant :

Gep S.p.A

Corso Salvatore D'Amato, 90
80022 Arzano, Naples
Italy

Les sites de développement du microcontrôleur sont identifiés dans le rapport de certification [CERT_IC].

1.2.5. Configuration évaluée

Le certificat porte sur la configuration « fermée » du produit.
Le produit testé par le centre d'évaluation est représentatif du produit final.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3 [CC]** et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

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 « P5CD080V0B » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 3 novembre 2010 sous la référence BSI-DSZ-CC-0680-2010 ([CERT_IC]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 juin 2011, 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 par rapport aux référentiels techniques de l'ANSSI n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités exploitables pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit est celui du microcontrôleur (voir le rapport de certification [CERT_IC]). L'évaluation n'a pas mis en évidence de vulnérabilités exploitables pour le niveau AVA_VAN 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 « Passeport electronique EAC PEACOS sur P5CD080 V0B, version 1.2 » 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, 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'accord[1], 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 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, 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 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	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 Support au cycle de vie	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	**4**	Problem tracking 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	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	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**	**1**	Testing: security enforcing modules
	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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « Security Target for the PEACOS Electronic Passport with Extended Access Control », référence TSRE090008, version 1.7. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security Target Lite for the PEACOS Extended Access Control MRTD », référence TCLE100138, version 1.2.
[RTE]	« Evaluation Technical Report MATISSE Project », référence MATISSE_ETR_V1.2, version 1.2
[CONF]	« Configuration Item List for the PEACOS Electronic Passport », référence TSRE100137, version 1.3.
[GUIDES]	Guide d'installation du produit : - « Initialization guidance for the PEACOS Electronic Passport », référence TSRE090016, version 1.2. Guide d'administration du produit : - « Personalization guidance for the PEACOS Electronic Passport », référence TSRE090017, version 1.2 Guide d'utilisation du produit : - « User Guidance for the PEACOS Electronic Passport », référence TSRE090011, version 1.1.
[CERT_IC]	Rapport de certification pour les microcontrôleurs NXP P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B associés à leurs logiciels dédiés. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-DSZ-CC-0680-2010.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001*.
[PP EAC]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.2, 19 Novembre 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026-2006-MA-01*.

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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002, version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001, version 2.7, revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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.