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-PP-2010/06 du profil de protection « Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control » (référence PP-MRTD-SAC/PACE V2, version 1.00)

Paris, le 3 novembre 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

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-PP-2010/06

Nom du profil de protection

Machine Readable Travel Document
SAC (PACE V2) Supplemental Access Control

Référence/version du profil de protection

Référence PP-MRTD-SAC/PACE V2 - version 1.00

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation imposé par le PP

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Rédacteur(s)

ANTS

5 rue de l'Eglise, 08000 Charleville-Mézières, France

Commanditaire

ANTS

5 rue de l'Eglise, 08000 Charleville-Mézières, France

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

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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Table des matières

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Protection Profile — Machine Readable Travel Document — SAC (PACE V2) Supplemental Access Control
Référence : PP-MRTD-SAC/PACE V2
Version : 1.00
Date : 21 septembre 2010

1.2. Rédacteur

Ce profil de protection a été rédigé par :

ANTS

5 rue de l'Eglise
08000 Charleville-Mézières
France

1.3. Description du profil de protection

La cible d'évaluation (TOE – *Target Of Evaluation*) définie dans ce PP correspond à un document de voyage électronique supportant le « *Supplemental Access Control* » défini par l'ICAO (cf. [ICAO – TR – SAC]).

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection sont les suivantes :

- concernant les fonctionnalités d'audit de sécurité :
  - Audit storage (FAU_SAS.1) ;
- concernant les fonctionnalités cryptographiques :
  - Cryptographic key generation – Generation of Document V2 Session Keys by the TOE (FCS_CKM.1);
  - Cryptographic key destruction – MRTD (FCS_CKM.4);
  - Cryptographic operation – Hash for Key Derivation (FCS_COP.1/SHA);
  - Cryptographic operation – Symmetric Encryption / Decryption (FCS_COP.1/ENC);
  - Cryptographic operation – Authentication (FCS_COP.1/AUTH);
  - Cryptographic operation – MAC (FCS_COP.1/MAC);
  - Quality metric for random numbers (FCS_RND.1);
- concernant les fonctionnalités d'identification et d'authentification :
  - Timing of identification (FIA_UID.1) ;
  - Timing of authentication (FIA_UAU.1);
  - Single-use authentication mechanisms (FIA_UAU.4);
  - Multiple authentication mechanisms (FIA_UAU.5);
  - Re-authenticating – Re-authenticating of Terminal by the TOE (FIA_UAU.6);

  - Authentication failure handling (FIA_AFL.1);
- concernant les fonctionnalités de protection des données utilisateur :
  - Subset access control – PACE V2 Access control (FDP_ACC.1);
  - Basic Security attribute based access control – PACE V2 Access Control (FDP_ACF.1);
  - Basic data exchange confidentiality – MRTD (FDP_UCT.1);
  - Data exchange integrity – MRTD (FDP_UIT.1);
- concernant les fonctionnalités de gestion de la sécurité :
  - Specification of Management Functions (FMT_SMF.1);
  - Security roles (FMT_SMR.1);
  - Limited capabilities (FMT_LIM.1);
  - Limited availability (FMT_LIM.2);
  - Management of TSF data – Writing of Initialization Data and Pre-personalization Data (FMT_MTD.1/INI_ENA);
  - Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data (FMT_MTD.1/INI_DIS);
  - Management of TSF data – Key Write (FMT_MTD.1/KEY_WRITE);
  - Management of TSF data – Key Read (FMT_MTD.1/KEY_READ);
- concernant les fonctionnalités de protection des fonctions de sécurité :
  - TOE Emanation (FPT_EMSEC.1) ;
  - Failure with preservation of secure state (FPT_FLS.1);
  - TSF testing (FPT_TST.1);
  - Resistance to physical attack (FPT_PHP.3);

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4 augmenté des composants d'assurance suivants**[1] :

Composants	Descriptions
ALC_DVS.2	Sufficiency of security measures
AVA_VAN.5	Advanced methodical vulnerability analysis

Tableau 1 - Augmentations

Toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

[1] Voir l'Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Commanditaire

ANTS

5 rue de l'Eglise
08000 Charleville-Mézières
France

2.3. Centre d'évaluation

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 75

Adresse électronique : e.francois@serma.com

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 octobre 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives aux composants d'assurance ci-dessous sont à « **réussite** ».

Composants	Descriptions
APE_CCL.1	Conformance claims
APE_ECD.1	Extended components definition
APE_INT.1	Protection profile introduction
APE_OBJ.2	Security objectives
APE_REQ.2	Derived security requirements
APE_SPD.1	Security problem definition

Tableau 2 - Evaluation du PP

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.

3.2. Recommandations et limitations d'usage

Le rédacteur d'une cible de sécurité doit tenir compte des différentes notes qui sont écrites à son intention dans ce [PP SAC]. En particulier la note d'application 11 relative à l'objectif sur la cible d'évaluation OT.Identification. Cette note impose au rédacteur d'une cible de sécurité conforme au [PP SAC] de vérifier que les applications coexistant avec le passeport électronique respectent également OT.Identification.

3.3. Reconnaissance européenne (SOG-IS)

Ce rapport de certification 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 :

3.4. Reconnaissance internationale (CC RA)

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

[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 Royaume-Uni et la Suède.

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], 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 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

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.	
[CPP/P/01]	Procédure CPP/P/01 Certification de profils de protection, 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 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.
[PP SAC]	Profil de Protection objet de ce rapport de certification : - Protection Profile - Machine Readable Travel Document - SAC (PACE V2) Supplemental Access Control ; Référence PP-MRTD-SAC/PACE V2, version 1.00, 21 September 2010.
[RTE]	Rapport d'évaluation technique : - Evaluation Technical Report - CC Protection Profile; Ref. : C10P0037_ETR_v2.1, version 2.1 V2, 8 octobre 2010 ; Serma Technologies
[ICAO – TR – SAC]	ICAO TR – Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, 23 March 2010