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-2010/01 du profil de protection « Electronic Purse Protection Profile » (référence SFPMEI-CC-PP-EP, version 1.5 du 4 février 2010)

Paris, le 17 février 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-2010/01

Nom du profil de protection

Electronic Purse Protection Profile

Référence/version du profil de protection

Référence SFPMEI-CC-PP-EP /
version 1.5 du 4 février 2010

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

Trusted Labs SAS
5 rue du Bailliage, 78000 Versailles, France

Commanditaires

BMS
153 rue Saint-Honoré, 75001 Paris, France

SFPMEI
168 rue de Rivoli, 75001 Paris, 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

Reconnaissance jusqu'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 :

- 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 : Electronic Purse Protection Profile.
Référence : SFPMEI-CC-PP-EP, version 1.5.
Date : 4 février 2010.

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs S.A.S.

5 rue du Bailliage
78000 Versailles
France

1.3. Description du profil de protection

La cible d'évaluation définie dans le profil de protection [PP] est un porte-monnaie électronique. Celui-ci intégre un microcircuit (qui devra être certifié par ailleurs conformément au profil de protection [PP-0035]) et l'ensemble des logiciels embarqués nécessaires à l'implémentation de ses fonctionnalités.

La cible d'évaluation décrite dans le profil de protection doit être capable de :
- stocker le montant de monnaie électronique qui définit le solde du porte-monnaie électronique ;
- indiquer le montant disponible dans le porte-monnaie électronique ;
- débiter la monnaie électronique par des opérations de débit ;
- créditer la monnaie électronique par des opérations de chargement et de chargement rapide ;
- mettre à jour les paramètres du porte-monnaie électronique.

La fonctionnalité première de la cible d'évaluation définie dans le profil de protection est de permettre au porteur du porte-monnaie électronique de réaliser des paiements d'une manière simple, sûre et rapide.

La cible d'évaluation doit fournir la possibilité de réaliser des paiements hors ligne, ce qui requiert les mécanismes de sécurité suivants pour se prémunir contre la fraude :
- protection en intégrité pendant le chargement, le chargement rapide et les opérations de débit ;
- protection en intégrité et en confidentialité des clés cryptographiques lorsqu'elles sont utilisées ou stockées ;
- authentification mutuelle entre la cible d'évaluation et le module d'accès sécurisé (*Secure Access Module* – SAM) pendant le chargement rapide et les opérations de débit ;
- authentification mutuelle entre la cible d'évaluation et les dispositifs de chargement pendant les opérations de chargement ;

- authentification du porteur du porte-monnaie électronique pendant les opérations de chargement et de chargement rapide.

1.4. Exigences fonctionnelles

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

- Audit data generation (FAU_GEN.1)
- Audit review (FAU_SAR.1)
- Protected audit trail storage (FAU_STG.1)
- Enforced proof of origin (FCO_NRO.2)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attribute based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Import of user data without security attributes (FDP_ITC.1)
- Stored data integrity monitoring (FDP_SDI.1)
- TSF Generation of secrets (FIA_SOS.2)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Re-authenticating (FIA_UAU.6)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Inter-TSF confidentiality during transmission (FPT_ITC.1)
- Inter-TSF detection and modification (FPT_ITI.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance of physical attack (FPT_PHP.3)
- Function recovery (FPT_RCV.4)
- Replay detection (FPT_RPL.1)

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. Commanditaires

BMS

153 rue Saint-Honoré
75001 Paris
France

SFPMEI

168 rue de Rivoli
75001 Paris
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 12 janvier 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives à la classe d'exigences d'assurance APE sont à « **réussite** ».

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. 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 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. Reconnaissance internationale (CC RA)

Ce rapport de certification 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 Royaume-Uni, 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
	ADO_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: basic 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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références

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.	
[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 2.0, April 1999, Management Committee of Agreement Group.
[PP-0035]	Security IC Platform Protection Profile, Référence : BSI-PP-0035, version 1.0 du 15/06/2007 *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0035-2007.*
[PP]	Electronic Purse Protection Profile, Référence : SFPMEI-CC-PP-EP, version 1.5 du 04/02/2010, Trusted Labs SAS
[RTE]	Electronic Purse and Secure Access Module for EM system Protection Profiles Evaluation Report, Référence: MONEO_APE_v1.2, version 1.2, Serma Technologies