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-2015/03 du profil de protection « Point of Interaction Protection Profile, POI-COMPREHENSIVE base PP » (version 4.0)

Paris, le 31 mars 2015

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

Guillaume POUPARD
[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-2015/03

Nom du profil de protection

Point of Interaction Protection Profile, POI-COMPREHENSIVE base PP

Référence/version du profil de protection

Point of Interaction Protection Profile, POI-COMPREHENSIVE base PP, version 4.0

Conformité à un profil de protection

Néant

PP-Base certifié

ANSSI-CC-PP-POI-COMPREHENSIVE

PP-Module associé aux PP-Configurations certifiées

ANSSI-CC-PP-POI-SRED-PP-Module

Critères d'évaluation et version

Critères Communs version 3.1, révision 4

Niveau d'évaluation imposé par le PP

EAL_POI - POI-COMPREHENSIVE

Rédacteurs

Security Research & Consulting GmbH
Graurheindorfer Strasse 149a,
D-53117 Bonn, Allemagne

SiVenture
Unit 6, Cordwallis Park,
Clivemont Road-Maidenhead
Berkshire SL6 7BU,
Royaume-Uni

Trusted Labs S.A.S.
6, rue de la Verrerie
92197 Meudon, France

Commanditaire

ANSSI
51 boulevard de La Tour-Maubourg, 75700 Paris 07 SP, France

Centre d'évaluation

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

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. PRESENTATION DU PROFIL DE PROTECTION 6

1.1. IDENTIFICATION DU PROFIL DE PROTECTION 6
1.2. REDACTEUR 6
1.3. DESCRIPTION DU PROFIL DE PROTECTION 6
1.3.1. Généralités 6
1.3.2. La configuration « POI-COMPREHENSIVE » 6
1.4. EXIGENCES FONCTIONNELLES 8
1.5. EXIGENCES D'ASSURANCE 8
1.6. CONFIGURATIONS EVALUEES 8

2. L'EVALUATION 9

2.1. REFERENTIELS D'EVALUATION 9
2.2. COMMANDITAIRE 9
2.3. CENTRE D'EVALUATION 9
2.4. TRAVAUX D'EVALUATION 9

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RECONNAISSANCE EUROPEENNE (SOG-IS) 11
3.3. RECONNAISSANCE INTERNATIONALE (CC RA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES 14

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Point of Interaction Protection Profile, POI-COMPREHENSIVE base PP [PP].
Version : 4.0.
Date : 6 mars 2015.

1.2. Rédacteur

Ce profil de protection a été rédigé par les intervenants suivants, dans le cadre d'un groupe de travail OSEC/JTEMS :

Security Research & Consulting GmbH	**SiVenture**	**Trusted Labs S.A.S.**
Graurheindorfer Strasse 149a, D-53117 Bonn, Allemagne	Unit 6, Cordwallis Park, Clivemont Road- Maidenhead Berkshire SL6 7BU, Royaume-Uni	6, rue de la Verrerie 92197 Meudon, France

1.3. Description du profil de protection

1.3.1. Généralités

Le groupe « *Common Approval Scheme* » (CAS) a pour but d'harmoniser les exigences de sécurité des systèmes de paiement européens dans le cadre du « *Single European Payment Area* » (SEPA). Dans ce contexte, il a rédigé un profil de protection pour les terminaux de paiement (PP POI[1]). Ce PP a été repris et est maintenu par le sous-groupe « *Joint Terminal Evaluation Method Subgroup* » (JTEMS) qui dépend du « *Joint Interpretation Working Group* » (JIWG) du SOG-IS.

Ce profil de protection décrit plusieurs configurations. Le présent rapport de certification ne traite que la configuration « POI-COMPREHENSIVE » ; les autres configurations sont certifiées par ailleurs.
Le PP « Point of Interaction Protection Profile, POI-PED-COMPREHENSIVE base PP » comprend un profil de protection de base, référencé ANSSI-CC-PP-POI-COMPREHENSIVE, auquel peut s'ajouter le PP-module optionnel « SRED PP Module », référencé ANSSI-CC-PP-POI-SRED-PP-Module. Les configurations évaluées sont définies dans le chapitre 1.6.

1.3.2. La configuration « POI-COMPREHENSIVE »

Le présent rapport décrit la configuration « POI-PED-COMPREHENSIVE », avec ou sans le module SRED optionnel, qui se concentre sur les modules de saisie du code confidentiel,

[1] POI : Point Of Interaction.

de l'affichage vers l'utilisateur, du lecteur de carte à puce, et de la sécurité du lecteur de bande magnétique, les modules de communication, de sécurité (hors code confidentiel), de séparation des applications et d'administration du terminal. Le périmètre de la TOE dans cette configuration est détaillé dans la figure 1.
Ce profil de protection ne réclame la conformité à aucun autre profil de protection.

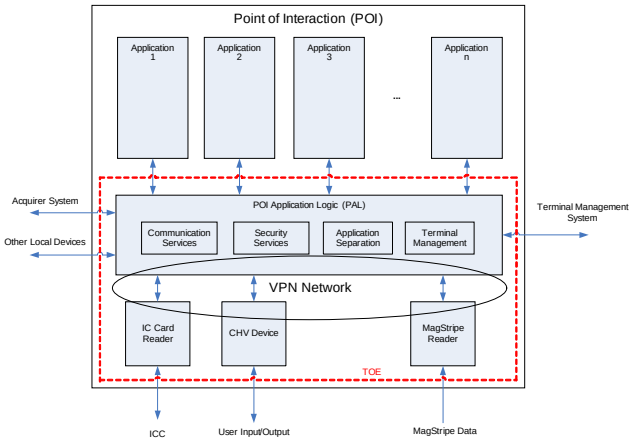

Figure 1 Configuration POI-COMPREHENSIVE

Une particularité de ce profil de protection est que les biens à protéger n'ont pas tous le même niveau de sensibilité et que le niveau de protection associé à ces biens est ajusté en conséquence. Cinq niveaux de protection ont ainsi été établis :

- basique ;
- faible ;
- faible renforcé ;
- moyen ;
- haut.

La figure 2 ci-dessous illustre cette notion sur les biens de la TOE « POI-COMPREHENSIVE ».

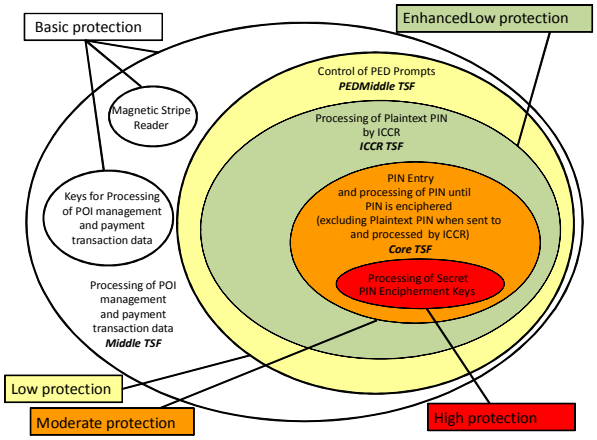

Figure 2 Niveaux de protection des biens et périmètres des configurations.

Dans le cas de recours au module SRED, certains biens changent de niveaux et font l'objet de mesures de protection renforcées.

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection[1] sont les suivantes :

- FCS_RND.1 Generation of random numbers;
- FPT_EMSEC.1 TOE emanation.

De plus, le profil de protection reprend des exigences fonctionnelles de sécurité définies dans la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Les **exigences d'assurance** définies par le profil de protection[2] sont les suivantes :

- AVA_POI.1/MSR ;
- AVA_POI.1/PEDMiddleTSF ;
- AVA_POI.2/MiddleTSF ;
- AVA_POI.1/ICCard ;
- AVA_POI.1/CoreTSF ;
- AVA_POI.1/CoreTSFKeys.

Toutes les autres exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC]. Ces exigences sont raffinées dans [CEM-POI]. Le niveau d'assurance exigé par le profil de protection est le niveau EAL_POI - POI-COMPREHENSIVE. Ce niveau d'assurance est défini en annexe 1.

1.6. Configurations évaluées

Deux PP-configurations ont été évaluées et sont certifiées :

1. Profil de protection de base : ANSSI-CC-PP-POI-COMPREHENSIVE ;
2. Profil de protection de base avec le PP-module « SRED PP Module » ANSSI-CC-PP-POI-COMPREHENSIVE + ANSSI-CC-PP-POI-SRED-PP-Module.

[1] Exigences fonctionnelles étendues non issues de la partie 2 des [CC].
[2] Exigences d'assurance étendues non issues de la partie 3 des [CC].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], ainsi qu'à l'addendum de ces deux méthodologies [Modular-PP].

2.2. Commanditaire

ANSSI

51 boulevard de La Tour-Maubourg,
75700 Paris 07 SP,
France

2.3. Centre d'évaluation

SERMA Technologies

14 rue Galilée
CS 10055
33615 Pessac Cedex
France

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 13 mars 2015 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** ».

Pour la configuration 1 (Profil de protection de base, voir le chapitre 1.6), les composants évalués (définis dans [CC]) sont les suivants :

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 3 - Evaluation du PP pour la configuration 1

Pour la configuration 2, (Profil de protection de base et PP-module SRED PP) les composants évalués (définis dans [Modular-PP]) sont les suivants :

Composants	Descriptions
ACE_CCL.1	Conformance claims
ACE_ECD.1	Extended components definition
ACE_INT.1	Protection profile introduction
ACE_OBJ.2	Security objectives
ACE_REQ.2	Derived security requirements
ACE_SPD.1	Security problem definition
ACE_MCO.1	PP-module consistency
ACE_CCO.1	PP-configuration consistency

Tableau 4 - Evaluation du PP pour la configuration 2

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 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 classes d'assurance APE et ACE. 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.

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[1], des certificats Critères Communs. La reconnaissance s'applique pour les classes d'assurance APE et ACE. 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

Security Assurance Requirements			EAL POI		
			PED-ONLY	POI-COMPREHENSIVE	POI-CHIP-ONLY and Open Protocol Package
EAL2	ADV_ARC.1	Raffiné	X	X	X
	ADV_FSP.2	Standard	X	X	X
	ADV_TDS.1	Standard	X	X	X
	AGD_OPE.1	Raffiné	X	X	X
	AGD_PRE.1	Standard	X	X	X
	ALC_CMC.2	Raffiné	X	X	X
	ALC_CMS.2	Raffiné	X	X	X
	ALC_DEL.1	Raffiné	X	X	X
	ATE_COV.1	Standard	X	X	X
	ATE_FUN.1	Standard	X	X	X
	ATE_IND.2	Raffiné	X	X	X
	ALC_DVS.2	Raffiné	X	X	X
	ALC_FLR.1	Raffiné	X	X	X
Extended Requirements	AVA_POI.1/MSR	Étendu	X	X	
	AVA_POI.1/PEDMiddleTSF	Étendu	X	X	X
	AVA_POI.2/MiddleTSF	Étendu		X	X
	AVA_POI.1/ICCard	Étendu	X	X	
	AVA_POI.1/CoreTSFKeys	Étendu	X	X	
	AVA_POI.1/CoreTSF	Étendu	X	X	X

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 ANSSI-CC-CPP-P-01 Certification de profils de protection, version 2 du 30 mai 2011. ANSSI.
[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.
[Modular-PP]	CC and CEM addenda - Modular PP, March 2014, version 1.0, ref CCDB-2014-03-001.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[RTE]	Evaluation Technical Report - PP_POI_v4 Project, référence PP_POI_v4_ETR_v1.1, version 1.1 du 13 mars 2015.
[PP]	Point of Interaction Protection Profile, version 4.0, 6 mars 2015.
[CEM-POI]	CEM Refinements for POI Evaluation, version 1.0, 27 mai 2011.