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-2010/08 du profil de protection « Point of Interaction Protection Profile » « POI-PED-ONLY » (version 2.0)

Paris, le 6 janvier 2011

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

Patrick Pailloux
[Original signé]

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-2010/08

Nom du profil de protection

Point of Interaction Protection Profile
« POI-PED-ONLY »

Référence/version du profil de protection

ANSSI-CC-PP-POI-PED-ONLY Version 2.0

Conformité à un profil de protection

Ce profil de protection ne réclame pas de conformité à un autre profil de protection.

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation imposé par le PP

EAL_POI

Rédacteur(s)

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

Trusted Labs S.A.S.
5, rue du Bailliage
78000 Versailles, France

Commanditaire

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

Centre d'évaluation

THALES - CEACI (T3S – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.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 : Point of Interaction Protection Profile « POI-PED-ONLY »
Version 2.0
Date : 26 novembre 2010

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs S.A.S.
5, rue du Bailliage
78000 Versailles, France

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

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). Ce PP a été repris et est maintenu par le sous groupe « *Joint Terminal Evaluation Method Subgroup* » (JTEMS) qui dépend de la « *Joint Interpretation Library* » (JIL).

Ce profil de protection décrit trois TOE matérielles correspondant à trois besoins identifiés par le groupe CAS

- « POI-PED-ONLY » ;
- « POI-COMPREHENSIVE » ;
- « POI-OPTION ».

1.3.2. La configuration « POI-PED-ONLY »

Le présent rapport décrit la configuration « POI-PED-ONLY » qui se concentre sur les modules de saisie du code confidentiel, de l'affichage vers l'utilisateur, du lecteur de carte à puce, et de la sécurité du lecteur de bande magnétique. Le périmètre de la TOE dans cette configuration est détaillé dans la figure 1.
Ce profil de protection ne réclame la conformité à un autre profil de protection.

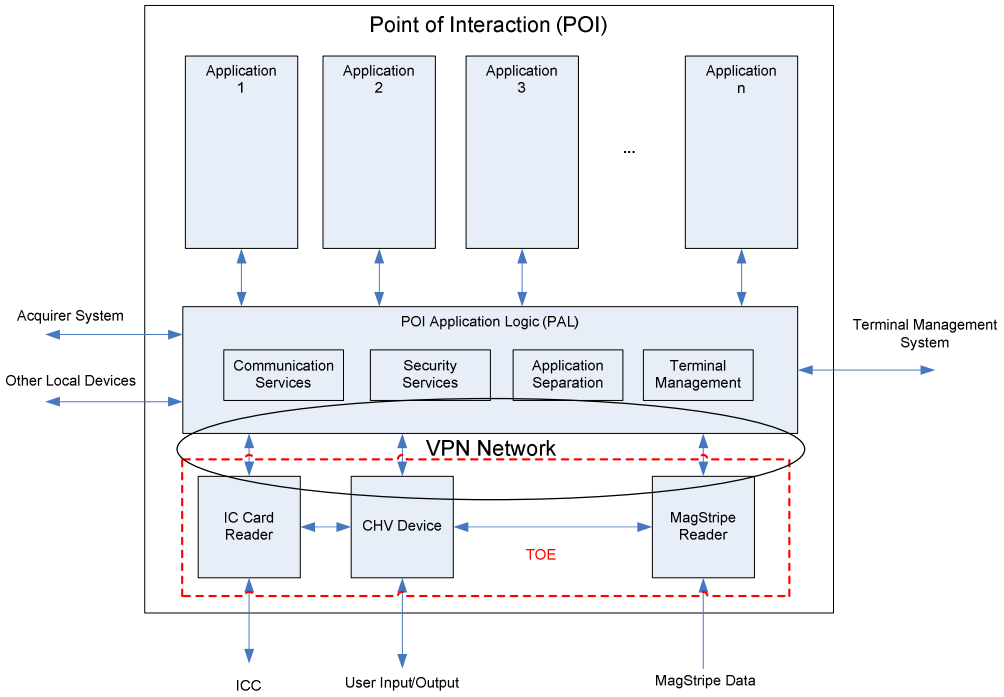

Figure 1 Configuration POI-PED-ONLY

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. Quatre niveaux de protection ont ainsi été établis :

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

La figure 4 ci-dessous illustre cette notion sur les biens de la TOE « POI-PED-ONLY ».

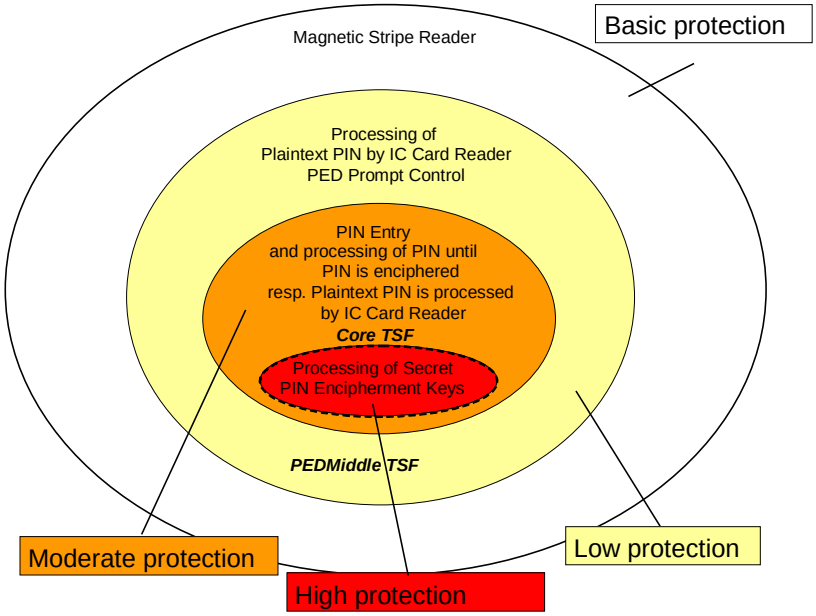

Figure 2 Niveaux de protection des biens et périmètres de la configuration « POI-PED-ONLY »

1.4. Exigences fonctionnelles

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

Package	SFR description	SFR
PIN_ENTRY	Subset information flow control	FDP_IFC.1/PIN_ENTRY
	Import of user data without security attributes	FDP_ITC.1/PIN_ENTRY
	User authentication before any action	FIA_UAU.2/PIN_ENTRY
	Timing of identification	FIA_UID.1/PIN_ENTRY
	TSF-initiated termination	FTA_SSL.3/PIN_ENTRY
	TOE Emanation	FPT_EMSEC.1/PIN_ENTRY
ENC_PIN	Subset information flow control	FDP_IFC.1/ENC_PIN
	Simple security attributes	FDP_IFF.1/ENC_PIN
	Basic internal transfer protection	FDP_ITT.1/ENC_PIN
	Subset residual information protection	FDP_RIP.1/ENC_PIN
	Entry Timing of identification	FIA_UID.1/ENC_PIN
	Management of security attributes	FMT_MSA.1/ENC_PIN
	Static attribute initialisation	FMT_MSA.3/ENC_PIN
	Security roles	FMT_SMR.1/ENC_PIN
	Trusted path	FTP_TRP.1/ENC_PIN
PLAIN_PIN	Subset information flow control	FDP_IFC.1/PLAIN_PIN
	Simple security attributes	FDP_IFF.1/PLAIN_PIN
	Basic internal transfer protection	FDP_ITT.1/PLAIN_PIN
	Subset residual information protection	FDP_RIP.1/PLAIN_PIN
	Entry Timing of identification	FIA_UID.1/PLAIN_PIN
	Management of security attributes	FMT_MSA.1/PLAIN_PIN
	Static attribute initialisation	FMT_MSA.3/PLAIN_PIN
	Security roles	FMT_SMR.1/PLAIN_PIN
IC Card Reader	Subset information flow control	FDP_IFC.1/ICCardReader
	Simple security attributes	FDP_IFF.1/ICCardReader
	Basic internal transfer protection	FDP_ITT.1/ICCardReader
	Subset residual information protection	FDP_RIP.1/ICCardReader
CoreTSF	Subset access control	FDP_ACC.1/CoreTSFLoader
	Import of user data without security attributes	FDP_ITC.1/CoreTSFLoader
	Failure with preservation of secure state	FPT_FLS.1/CoreTSF
	TSF testing	FPT_TST.1/CoreTSF
PEDMiddleTSF	Subset access control	FDP_ACC.1/PEDMiddleTSFLoader
	Import of user data without security attributes	FDP_ITC.1/PEDMiddleTSFLoader
	Failure with preservation of secure state	FPT_FLS.1/PEDMiddleTSF
	TSF testing	FPT_TST.1/PEDMiddleTSF
PED Prompt Control	Subset access control	FDP_ACC.1/PEDPromptControl
	Security attribute based access control	FDP_ACF.1/PEDPromptControl
Cryptography	Cryptographic operation	FCS_COP.1
	Quality metric for random numbers	FCS_RND.1
	trusted channel	FDP_ITC.1
	Import of user data with security attributes	FTP_ITC.2
	basic TSF data consistency	FPT_TDC.1
Physical Protection	TOE Emanation	FPT_EMSEC.1/CoreTSF
	Resistance to physical attack	FPT_PHP.3/CoreTSF
	Resistance to physical attack	FPT_PHP.3/ICCardReader
	Resistance to physical attack	FPT_PHP.3/MSR

Tableau 1 Liste des SFR selon les packages définis dans le PP

Les exigences fonctionnelles du profil de protection sont liées à la partie 2 des Critères Communs [CC] soit :

- directement ;
- après raffinement (opérations sur l'exigence fonctionnelle partiellement ou complètement réalisées) ;
- par extension.

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau EAL_POI. Ce niveau d'assurance est défini par les composants d'assurances suivants :

Exigence d'assurance	Opération	EAL POI / PED-ONLY
ADV_ARC.1	Raffiné	X
ADV_FSP.2	Standard	X
ADV_TDS.1	Standard	X
AGD_OPE.1	Raffiné	X
AGD_PRE.1	Standard	X
ALC_CMC.2	Raffiné	X
ALC_CMS.2	Raffiné	X
ALC_DEL.1	Raffiné	X
ATE_COV.1	Standard	X
ATE_FUN.1	Standard	X
ATE_IND.2	Standard	X
ALC_DVS.2	Raffiné	X
AVA_POI.1/MSR	Étendu	X
AVA_POI.2/PEDMiddleTSF	Étendu	X
AVA_POI.2/MiddleTSF	Étendu	
AVA_POI.3/CoreTSF	Étendu	X
AVA_POI.4/CoreTSFKeys	Étendu	X

Tableau 2 – EAL_POI

Les exigences d'assurance du profil de protection sont liées à la partie 3 des Critères Communs [CC] soit :

- directement ;
- après raffinement (précisions sur l'exigence d'assurance) ;
- par extension.

2. L'évaluation

2.1. Référentiels d'évaluation

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

La partie 2 du référentiel CC est étendue avec les classes fonctionnelles de sécurité

- FCS_RND « *Generation of random numbers* » ;
- FPT_EMSEC « *TOE emanation* » ;
- FIA_API « *Authentication Proof of Identity* ».

La partie 3 du référentiel CC est étendue avec la famille d'assurance AVA_POI composée de :

- AVA_POI.1/MSR ;
- AVA_POI.2/PEDMiddleTSF ;
- AVA_POI.2/MiddleTSF ;
- AVA_POI.3/CoreTSF ;
- AVA_POI.4/CoreTSFKeys.

2.2. Commanditaire

ANSSI

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

2.3. Centre d'évaluation

THALES – CEACI (T3S – CNES)

18 avenue Edouard Belin
BPI1414
31401 Toulouse Cedex 9
France

Téléphone : +33 (0)5 62 88 28 01 ou 18

Adresse électronique : nathalie.feyt@thalesgroup.com

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 novembre 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 3 - 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. 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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. 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, 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

Security Assurance Requirements		EAL POI		
		PED-ONLY	POI-COMPREHENSIVE	POI-OPTION
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	Standard	X	X	X
ALC_DVS.2	Raffiné	X	X	X
AVA_POI.1/MSR	Étendu	X	X	
AVA_POI.2/PEDMiddleTSF	Étendu	X	X	X
AVA_POI.2/MiddleTSF	Étendu		X	X
AVA_POI.3/CoreTSF	Étendu	X	X	X
AVA_POI.4/CoreTSFKeys	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 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.
[POI CEM]	Terminal Evaluation Methodology – CEM refinement, version 1.0, du 30 janvier 2010.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[RTE]	Protection Profile evaluation detailed technical report. Project: PP POI, référence POI_APE, version 4.0 du 29 novembre 2010.