Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-PP-2009/02
Protection Profile
Embedded Software for Smart Secure Devices
Basic and Extended Configurations
(référence ANSSI-CC-PP-ESforSSD, version 1.0 du 27 novembre 2009)

Paris, le 1er décembre 2009

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 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-2009/02**
Nom du profil de protection ***Protection profile*** ***Embedded Software for Smart Secure Devices*** ***Basic and Extended Configurations***
Référence/version du profil de protection **ANSSI-CC-PP-ESforSSD,** **version 1.0 du 27 novembre 2009**
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) **Trusted Labs SAS** **5 rue du Bailliage, 78000 Versailles, France**
Commanditaire **ANSSI** **51, boulevard de la Tour-Maubourg ,75700 Paris 07 SP, France**
Centre d'évaluation **CEA - LETI** **17 rue des martyrs, 38054 Grenoble Cedex 9, France** **Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr**
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, 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

Ce [PP] est un document unique regroupant deux profils de protection sous la forme de deux configurations, chacune étant identifiable de manière unique :

- ANSSI-CC-PP-ESforSSD_Basic pour la configuration *Basic* (de base) ;
- ANSSI-CC-PP-ESforSSD_Extended pour la configuration *Extended* (étendue) ;

Le document est organisé de façon à identifier aisément les éléments spécifiques à chaque configuration, comme les chapitres, figures ou tables : ils sont marqués d'une étiquette (ANSSI-CC-PP-ESforSSD_Basic ou ANSSI-CC-PP-ESforSSD_Extended) identifiant la configuration ; les éléments communs aux deux configurations ne portent pas d'étiquette.

Les deux tables ci-après récapitulent les caractéristiques de chaque configuration :

Titre	*Protection profile* *Embedded Software for Smart Secure Devices* *Basic Configuration*
Identifiant de la configuration	ANSSI-CC-PP-ESforSSD_Basic
Référence du document	ANSSI-CC-PP-ESforSSD
Version du document	1.0
Date du document	27 novembre 2009
Version CC	CCv3.1r3
Rédacteur	Trusted Labs SAS
Commanditaire	ANSSI

Titre	*Protection profile* *Embedded Software for Smart Secure Devices* *Extended Configuration*
Identifiant de la configuration	ANSSI-CC-PP-ESforSSD_Extended
Référence du document	ANSSI-CC-PP-ESforSSD
Version du document	1.0
Date du document	27 novembre 2009
Version CC	CCv3.1r3
Rédacteur	Trusted Labs SAS
Commanditaire	ANSSI

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs SAS

5 rue du Bailliage, 78000 Versailles, France

1.3. Description du profil de protection

Le présent [PP] remplace le précédent [PP 9911] intitulé *Smart Card Integrated Circuit with Embedded Software* qui a été certifié par l'ANSSI en 1999.

Ce [PP] répond au besoin de disposer d'une expression des exigences de sécurité correspondant aux tendances actuelles en matière de développements de produits *smart secure devices* (dispositifs sécurisés intelligents), dont la carte à puce est un exemple type. En effet, il est le résultat de la collaboration des principaux acteurs concernés par ce [PP], c'est-à-dire les développeurs de produits se référant à ce type de [PP], les donneurs d'ordre commandant ce type de produit et les évaluateurs de ce type de produit.

Ce [PP] s'applique aux produits *smart secure devices* composés d'un composant électronique sécurisé (*Security IC*) embarquant du logiciel de type système d'exploitation (*native OS – Operating System*). Le composant fournit le processeur, les dispositifs de sécurité, le générateur d'aléa, les ports d'entrée et de sortie, les mémoires volatiles et non volatiles. Le logiciel implémente les fonctionnalités du système d'exploitation telles que le démarrage sécurisé, la gestion de la mémoire, la gestion du cycle de vie et, le cas échant, des fonctionnalités ou comportements applicatifs.

Les produits visés par le [PP] sont de deux types :

- les produits intégrés, dans lesquels le logiciel, élaboré en langage natif, comprend à la fois le code du système d'exploitation et celui de l'applicatif, les deux étant imbriqués ;
- les produits en couches, dans lesquels le logiciel est constitué de deux couches superposées :
    - une couche logicielle basse - couche système d'exploitation - contenant le code du système d'exploitation et, éventuellement, comportant du code applicatif ;
    - une couche logicielle haute - couche applicative - contenant le code des applications ; celles-ci s'appuient sur les fonctionnalités offertes par le système d'exploitation ; ce dernier fournit également un mécanisme de séparation entre la couche applicative et la couche système d'exploitation.

Ce [PP] fixe les exigences de sécurité qui s'imposent uniquement au système d'exploitation, celui-ci constituant pour ce [PP] la cible d'évaluation (*Target Of Evaluation* - TOE) ; le composant est considéré comme un environnement pour le système d'exploitation, et est couvert par des objectifs de sécurité. Cependant, toute évaluation d'un produit *smart secure device* réclamant une conformité à ce [PP] doit comprendre le produit complet, c'est-à-dire le composant et le système d'exploitation qui y est embarqué. La cible de sécurité (*Security Target* - ST) du produit doit comporter des objectifs de sécurité pour le composant sous-jacent correspondant aux exigences de sécurité pour le composant décrites dans ce [PP]. Ce principe fait partie d'un ensemble de principes qui ont été adoptés pour ce [PP], et qui sont détaillés dans le [PP], notamment au chapitre *4 Underlying security model*.

L'évaluation du produit peut être faite en mode « composition », en respectant les exigences d'assurance de sécurité décrites dans [COMP][1], pourvu que le composant ait été évalué séparément. Concernant cette dernière évaluation, ce [PP] n'exige pas de conformité du composant à un profil de protection particulier (dédié aux composants), mais il est à noter que les composants évalués selon le [PP0035] répondent complètement aux objectifs. Toutefois, la composition avec un composant déjà certifié n'est pas obligatoire. Dans le cas où le composant n'a pas été évalué, l'évaluation du produit doit couvrir à la fois le composant et le système d'exploitation. Les exigences en matière d'analyse de vulnérabilité que l'on trouve dans le document [CC AP] s'appliquent dans les deux cas (évaluation en composition ou évaluation d'un coup).

Ce [PP] définit deux types de configuration pour la TOE, *Basic* et *Extended*, correspondant aux deux types de produits identifiés plus haut :

- *Basic TOE :* il n'y a pas de séparation entre le système d'exploitation et les applications ; la *Basic TOE* implémente des caractéristiques de sécurité pour ses propres besoins (voir chapitre 2.4.1 du [PP]) ; cette configuration correspond aux produits intégrés ;
- *Extended TOE* : le système d'exploitation fournit un mécanisme de séparation entre la couche applicative et la couche système d'exploitation ; la *Extended TOE* implémente des caractéristiques de sécurité pour ses propres besoins et éventuellement pour la couche applicative (voir chapitre 2.4.2 du [PP]) ; cette configuration correspond aux produits en couches.

Chacune des deux configurations pour la TOE donne lieu à un profil de protection à part entière, chacun portant un identifiant unique :

- ANSSI-CC-PP-ESforSSD_Basic s'adresse aux produits intégrés avec une *Basic TOE* dans laquelle le système d'exploitation et les applications sont imbriqués ;
- ANSSI-CC-PP-ESforSSD_Extended s'adresse aux produits en couches avec une *Extended TOE* dans laquelle le système d'exploitation fournit un mécanisme de séparation entre la couche applicative et la couche système d'exploitation.

Ce [PP] requiert une conformité démontrable.

Les cibles de sécurité ou les profils de protection conformes à ce [PP] peuvent élargir le périmètre de la TOE, suivant la configuration choisie, en adjoignant des fonctionnalités additionnelles comme, par exemple, des mécanismes d'authentification, des mécanismes de chargement de code ou de données après la délivrance de la TOE, ou encore des protocoles de communications sécurisées[2].

[1] Les exigences d'assurance de sécurité que l'on trouve dans [COMP] s'ajoutent à celles correspondant à l'EAL (*Evaluation Assurance Level*) spécifié dans le présent [PP], en particulier les exigences concernant les recommandations issues de l'évaluation du composant.

[2] Ce [PP] a été conçu de façon à faciliter les évaluations en composition avec un profil de protection, dédié à une application, comme celui pour le porte-monnaie électronique [PPEP] ou encore celui pour *Java Card System* [PPJCS].

1.4. Exigences fonctionnelles

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

- concernant la TOE en configuration *Basic* :
  - relativement à la fonctionnalité d'atomicité (*atomicity*) :
    - *FDP_ACC.1/Atomicity Subset access control ;*
    - *FDP_ROL.1/Atomicity Basic rollback ;*
  - relativement à la fonctionnalité de confidentialité (*confidentiality*) :
    - *FDP_ACC.1/Confidentiality Subset access control ;*
    - *FDP_ACF.1/Confidentiality Security attribute based access control ;*
    - *FDP_RIP.1/Confidentiality Subset residual information protection ;*
    - *FDP_UCT.1/Confidentiality Basic data exchange confidentiality ;*
    - *FMT_MSA.1/Confidentiality Management of security attributes ;*
    - *FMT_MSA.3/Confidentiality Static attribute initialisation ;*
    - *FPR_UNO.1/Confidentiality Unobservability ;*
    - *FPT_ITC.1/Confidentiality Inter-TSF confidentiality during transmission ;*
  - relativement à la fonctionnalité de cryptographie (c*ryptography*) :
    - *FCS_CKM.4 Cryptographic key destruction ;*
    - *FCS_COP.1 Cryptographic operation ;*
  - relativement à la fonctionnalité d'intégrité (*integrity*) :
    - *FDP_ACC.1/Integrity Subset access control ;*
    - *FDP_ACF.1/Integrity Security attribute based access control ;*
    - *FDP_SDI.2/Integrity Stored data integrity monitoring and action ;*
    - *FDP_UIT.1/Integrity Data exchange integrity ;*
    - *FMT_MSA.1/Integrity Management of security attributes ;*
    - *FMT_MSA.3/Integrity Static attribute initialisation ;*
    - *FPT_ITI.1/Integrity Inter-TSF detection of modification ;*
  - relativement à la fonctionnalité de gestion du cycle de vie (*life cycle*) :
    - *FDP_ACC.1/Life_cycle Subset access control ;*
    - *FDP_ACF.1/Life_cycle Security attribute based access control ;*
    - *FMT_MSA.1/Life_cycle Management of security attributes ;*
    - *FMT_MSA.3/Life_cycle Static attribute initialisation ;*
  - relativement à la fonctionnalité de supervision (*monitoring*) :
    - *FAU_ARP.1/Monitoring Security alarms ;*
    - *FAU_SAA.1/Monitoring Potential violation analysis ;*
  - relativement à la fonctionnalité d'exécution (*operate*) :
    - *FMT_MOF.1/Operate Management of security functions behaviour ;*
    - *FMT_MTD.1/Operate Management of TSF data ;*
    - *FPT_FLS.1/Operate Failure with preservation of secure state ;*
    - *FPT_TST.1/Operate TSF testing ;*
  - relativement à la fonctionnalité de nombres aléatoires (*random numbers*) :
    - *FIA_SOS.2/RND TSF Generation of secrets ;*
  - relativement à la fonctionnalité des rôles (*roles*) :
    - *FIA_UID.1 Timing of identification ;*
    - *FMT_SMR.1 Security roles ;*

- concernant la TOE en configuration *Extended :*
  - relativement à la fonctionnalité de séparation (*separation*) :
    - *FDP_IFC.1/Separation Subset information flow control ;*
    - *FDP_IFF.1/Separation Simple security attributes ;*
    - *FMT_MSA.3/Separation Static attribute initialisation ;*
    - *FMT_MSA.1/Separation Management of security attributes ;*

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

ANSSI

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

2.3. Centre d'évaluation

CEA - LETI

17 rue des martyrs
38054 Grenoble Cedex 9
France

Téléphone : +33 (0)4 38 78 40 87

Adresse électronique : cesti.leti@cea.fr

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 septembre 2009, 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. Conclusions

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

Comme indiqué plus haut (cf. 1.3 Description du profil de protection), le rédacteur d'une cible de sécurité réclamant une conformité à ce [PP] doit élaborer des objectifs de sécurité pour le composant sous-jacent correspondant aux exigences de sécurité pour le composant décrites dans ce [PP]. Ce principe fait partie d'un ensemble de principes qui ont été adoptés pour ce [PP], et qui sont détaillés dans le [PP], notamment au chapitre *4 Underlying security model*.

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 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle 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 :

3.4. 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 mutuelle 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_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 procedure
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 Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
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**	Independant 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.
[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 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, ou version courante applicable
[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]	Profil de protection objet du présent rapport de certification : Protection Profile - Embedded Software for Smart Secure Devices - Basic and Extended Configurations Référence ANSSI-CC-PP-ESforSSD, version 1.0 du 27 novembre 2009
[PP 9911]	Profil de protection certifié par l'ANSSI : Smart Card Integrated Circuit with Embedded Software Protection Profile, Version 2.0, June 1999
[PP0035]	Profil de protection certifié par le BSI : Security IC Platform Protection Profile, Version 1.0, June 2007
[RTE]	PROJECT PP-09x - Rapport de tâche APE Référence: LETI.CESTI.P9x.RAP.001 - v1.2 - 15/09/09