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-2020/01 du profil de protection « PC Client Specific TPM »

(TPM Library specification Family "2.0", Level 0, Revision 1.38, Version 1.2)

Paris, le 9 juin 2020

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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-PP-2020/01**
Nom du profil de protection **PC Client Specific TPM**
Référence/version du profil de protection **TPM Library specification Family “2.0”, Level 0, Revision 1.38, Version 1.2**
Conformité à un profil de protection **Néant**
PP-Base certifiée **Néant**
PP-Modules associés aux PP-Configurations certifiées **Néant**
Critères d’évaluation et version **Critères Communs version 3.1, révision 5**
Niveau d’évaluation imposé par le PP **EAL 4 augmenté** **ALC_FLR.1, AVA_VAN.4**
Rédacteur **Trusted Computing Group** **3855 SW 153rd Drive** **Beaverton, OR 97006, U.S.A**
Commanditaire **Trusted Computing Group** **3855 SW 153rd Drive** **Beaverton, OR 97006, U.S.A.**
Centre d’évaluation **THALES /CNES** **290 allée du Lac, 31670 Labège, 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. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : PC Client Specific TPM
Référence : TPM Library specification Family "2.0", Level 0, Revision 1.38
Version : Version 1.2
Date : 13 juin 2019

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
U.S.A

1.3. Description du profil de protection

Le profil de protection a été rédigé par le groupe de travail *Trusted Platform Module* du *Trusted Computing Group*.
Le *Trusted Computing Group* est une organisation à but non lucratif formée pour développer, définir et promouvoir des standards industriels ouverts supportant une racine de confiance matérielle pour l'interopérabilité de plateformes de confiance.

Le TPM, *Trusted Platform Module*, ou module de plateforme de confiance, est un composant électronique avec un logiciel embarqué. Il est destiné à être intégré dans des ordinateurs qui implémentent les fonctionnalités TCG PC Client Specific Trusted Platform Module (PCCS TPM) selon les spécifications du TPM 2.0 level 0 revision 1.38.

1.4. Exigences fonctionnelles

L'**exigence fonctionnelle de sécurité** définie par le profil de protection[1] est la suivante :

- *Random numbers generation* (FCS_RNG.1).

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

- *Selected proof of origin* (FCO_NRO.1) ;
- *Cryptographic key generation* (FCS_CKM.1) ;
- *Cryptographic key destruction* (FCS_CKM.4) ;
- *Cryptographic operation* (FCS_COP.1) ;

[1] Exigences fonctionnelles étendues non issues de la partie 2 des [CC].

- *Subset access control* (FDP_ACC.1) ;
- *Complete access control* (FDP_ACC.2) ;
- *Security attribute based access control* (FDP_ACF.1) ;
- *Export of user data without security attributes* (FDP_ETC.1) ;
- *Export of user data with security attributes* (FDP_ETC.2) ;
- *Import of user data without security attributes* (FDP_ITC.1) ;
- *Import of user data with security attributes* (FDP_ITC.2) ;
- *Subset residual information protection* (FDP_RIP.1) *;*
- *Stored data integrity monitoring* (FDP_SDI.1) ;
- *Basic data exchange confidentiality* (FDP_UCT.1) ;
- *Data exchange integrity* (FDP_UIT.1) ;
- *Basic Internal Transfer Protection* (FDP_ITT.1) ;
- *Authentication failures* (FIA_AFL.1) ;
- *TSF Generation of secrets* (FIA_SOS.2) ;
- *Timing of authentication* (FIA_UAU.1) ;
- *Multiple authentication mechanisms* (FIA_UAU.5) *;*
- *Re-authenticating* (FIA_UAU.6) ;
- *Timing of identification* (FIA_UID.1) ;
- *User-subject binding* (FIA_USB.1) ;
- *Management of security functions behavi*or (FMT_MOF.1) ;
- *Management of security attributes* (FMT_MSA.1) ;
- *Secure security attributes* (FMT_MSA.2) ;
- *Static attribute initialization* (FMT_MSA.3) ;
- *Security attribute value inheritance* (FMT_MSA.4) ;
- *Management of TSF data* (FMT_MTD.1) ;
- *Security roles* (FMT_SMR.1) ;
- *Specification of management Functions* (FMT_SMF.1) ;
- *Failure with preservation of secure state* (FPT_FLS.1) ;
- *Resistance to physical attacks* (FPT_PHP.3) ;
- *Reliable time stamps* (FPT_STM.1) ;
- *TSF testing* (FPT_TST.1) ;
- *Inter-TSF trusted channel* (FTP_ITC.1).

1.5. Exigences d’assurance

Le niveau d’assurance exigé par le profil de protection est le niveau **EAL4 augmenté des composants d'assurance ALC_FLR.1** et **AVA_VAN.4**.

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

La reconnaissance CCRA des produits évalués selon ce profil de protection sera limitée à EAL2.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Commanditaire

TRUSTED COMPUTING GROUP
3855 SW 153rd Drive
Beaverton, OR 97006
U.S.A.

2.3. Centre d'évaluation

THALES / CNES
290 Allée du lac
31670 Labège
France

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 12 mai 2020, 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** ».

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 1 - 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[2], des certificats ITSEC et Critères Communs. La reconnaissance européenne s’applique, pour la classe d’assurance APE. 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[3], des certificats Critères Communs. La reconnaissance s’applique pour la classe d’assurance APE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[2] La liste des pays signataires de l’accord SOG-IS est disponible sur le site web de l’accord : www.sogis.org.
[3] La liste des pays signataires de l’accord CCRA est disponible sur le site web de l’accord : www.commoncriteriaportal.org.

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 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	**1**	Identification of security measures
	ALC_FLR								**1**	Basic Flaw Remediation
	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	**4**	Moderate 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.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l’information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[PP]	Protection Profile PC Client Specific TPM, TPM Library specification Family “2.0”, Level 0, revision 1.38, version 1.2, 13 juin 2019, *TRUSTED COMPUTING GROUP*.
[RTE]	Evaluation Technical Report Project: TPM Protection Profile, version 1.0, reference TPM_2020_APE / Revision: 1.0, 12 mai 2020, *THALES/ CNES*.