



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**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-2021/02**

### **Profil de protection PC Client Specific TPM (PP PCCS TPM F2.0 L0 r1.59 V1.3)**

Paris, le 30 novembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]



## 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](mailto:certification@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	<b>ANSSI-CC-PP-2021/02</b>
Nom du profil de protection	<b>Profil de protection PC Client Specific TPM</b>
Référence/version du profil de protection	<b>PP PCCS TPM F2.0 L0 r1.59 V1.3</b>
Conformité à un profil de protection	Néant
PP-Base certifiée	Profil de protection de base
PP-Modules associés aux PP-Configurations certifiées	« ECDA A Optional Package »
Critère d'évaluation et version	<b>Critères Communs version 3.1 révision 5</b>
Niveau d'évaluation imposé par le PP	<b>EAL 4 augmenté</b> ALC_FLR.1, AVA_VAN.4
Rédacteur	<b>TRUSTED COMPUTING GROUP</b> 3855 SW 153rd Drive, Beaverton, OR 97003, USA
Commanditaire	<b>TRUSTED COMPUTING GROUP</b> 3855 SW 153rd Drive, Beaverton, OR 97003, USA
Centre d'évaluation	<b>THALES / CNES</b> 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables	 

## PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 disponibles sur le site Internet [www.ssi.gouv.fr](http://www.ssi.gouv.fr).

## TABLE DES MATIERES

1	Le profil de protection.....	6
1.1	Identification du profil de protection.....	6
1.2	Rédacteur .....	6
1.3	Description du profil de protection .....	6
1.4	Exigences fonctionnelles.....	6
1.5	Exigences d'assurance .....	7
1.6	Configurations évaluées.....	8
2	L'évaluation.....	9
2.1	Référentiels d'évaluation .....	9
2.2	Travaux d'évaluation .....	9
3	La certification .....	11
3.1	Conclusion.....	11
3.2	Reconnaissance du certificat.....	11
3.2.1	Reconnaissance européenne (SOG-IS).....	11
3.2.2	Reconnaissance internationale critères communs (CCRA).....	11
ANNEXE A.	Références .....	12
ANNEXE B.	Références liées à la certification .....	13

## 1 Le profil de protection

### 1.1 Identification du profil de protection

Titre : *Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 Version 1.3*

Référence, version : PP PCCS TPM F2.0 L0 r1.59 V1.3

Date : 29 septembre 2021

### 1.2 Rédacteur

Ce profil de protection a été rédigé par :

**TRUSTED COMPUTING GROUP**

3855 SW 153<sup>rd</sup> Drive,

Beaverton, OR 97003,

Etats Unis d'Amérique

### 1.3 Description du profil de protection

Le profil de protection a été rédigé par le groupe de travail *Trusted Platform Module* du TRUSTED COMPAGNY GROUP.

Le TRUSTED COMPAGNY 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 1.59.

Ce profil de protection autorise plusieurs configurations. En effet, il contient une partie « de base » qui consiste à définir des exigences de sécurités minimales, puis un PP-module optionnel « *ECDAA optional package* » correspondant à un schéma de signatures anonymisées ou pseudo-anonymisées. Les configurations évaluées sont définies dans le chapitre 1.6.

### 1.4 Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection<sup>1</sup> sont les suivantes :

- *Generation of random numbers* (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] :

---

<sup>1</sup> Exigences fonctionnelles étendues non issues de la partie 2 des [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) ;
- *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 behavior* (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 **EAL 4 augmenté des composants d'assurance suivants AVA\_VAN.4, ALC\_FLR.1**.

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.

## 1.6 Configurations évaluées

Deux PP-configurations ont été évaluées et sont certifiées :

1. Profil de protection de base ;
2. Profil de protection de base avec le PP-module « *ECDAA Optional Package* ».



## 2 L'évaluation

### 2.1 Référentiels d'évaluation

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

### 2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 octobre 2021, 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	<i>Conformance claims</i>
APE_ECD.1	<i>Extended components definition</i>
APE_INT.1	<i>Protection profile introduction</i>
APE_OBJ.2	<i>Security objectives</i>
APE_REQ.2	<i>Derived security requirements</i>
APE_SPD.1	<i>Security problem definition</i>

**Tableau 1 - Evaluation du PP pour la configuration 1**

Pour la configuration 2 (Profil de protection de base et module ECDA), les composants évalués sont les suivants :

Composants	Descriptions
ACE_CCL.1	<i>PP-module conformance claims</i>
ACE_ECD.1	<i>PP-module Extended components definition</i>
ACE_INT.1	<i>PP-module introduction</i>
ACE_OBJ.1	<i>PP-module objectives</i>
ACE_REQ.1	<i>PP-module security functional requirements</i>
ACE_SPD.1	<i>PP-module Security problem definition</i>
ACE_MCO.1	<i>PP-module consistency</i>
ACE_CCO.1	<i>PP-module configuration consistency</i>

**Tableau 2 - Evaluation du PP pour les configurations 2**

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

### 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 du certificat

##### 3.2.1 Reconnaissance européenne (SOG-IS)

Ce certificat 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<sup>2</sup>, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour classes d'assurance APE et ACE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



##### 3.2.2 Reconnaissance internationale critères communs (CCRA)

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires<sup>3</sup>, 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 :



---

<sup>2</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.eu](http://www.sogis.eu).

<sup>3</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org).

## ANNEXE A. Références

[PP]	<i>Protection Profile PC Client Specific Trusted Platform Module, TPM Library specification Family "2.0, Level 0, revision 1.59, version 1.3, 29 septembre 2021, TRUSTED COMPUTING GROUP.</i>
[RTE]	<i>Evaluation Technical Report Project : TCG TPM2.0 PP v1.3, TCG_TPM_PP_ETR / Revision:1.0, 28 octobre 2021, THALES / CNES.</i>

## ANNEXE B. Références liées à la certification

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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01 version 4.0.
[CC]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none"><li>- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;</li><li>- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;</li><li>- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li></ul>
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.