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 / Certification report

EUCC-3090-2026-26

Protection Profile PC Client Specific TPM
(PP PCCS TPM F2.0 V2.0)

Paris, le 26/4/2026 | 17:47 CEST

Vincent Strubel

SÉCURITÉ CERTIFICATION

AVERTISSEMENT / *WARNING*

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 de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

This report confirms that the evaluated version of the protection profile meets the evaluation criteria.

A protection profile is a public document that defines, for a product category, a set of security requirements and objectives, independent of their implementation, that meet the common security needs of a group of users.

Toute correspondance relative à ce rapport doit être adressée au :

All correspondence related to this report must be sent to:

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

PREFACE / *FOREWORD*

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 ;
- Les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits 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).

Certification of the security provided by information technology products and systems is governed by amended Decree 2002-535 of April 18th, 2002. This decree states that:

- *The Agence nationale de la sécurité des systèmes d'information drafts the certification reports. These reports specify the characteristics of the proposed security objectives. They may include any warnings authors deem necessary to mention for security reasons.*
- *The certificates issued by the Director General of ANSSI certify that the specific product or system submitted for evaluation meets the defined security characteristics. They also confirm that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (Article 8).*

Ce rapport est conforme à [EUCC].
This report is in compliance with [EUCC].

Les procédures de certification sont disponibles sur le site Internet https://www.cyber.gouv.fr/.

The certification procedures are available on the website www.cyber.gouv.fr.

TABLE DES MATIERES / *TABLE OF CONTENT*

1 Résumé / *Summary* 5
2 Le profil de protection / *Protection profile* 7
2.1 Identification du profil de protection / *Identification of the protection profile* 7
2.2 Rédacteur / Author 7
2.3 Description du profil de protection / *Description of the protection profile* 7
2.4 Exigences fonctionnelles / functional requirements 8
2.5 Exigences d'assurance / Assurance requirements 9
2.6 Contacts du PP / *PP contacts* 9
3 L'évaluation / *Evaluation* 10
3.1 Référentiels d'évaluation / *Evaluation reference bases* 10
3.2 Travaux d'évaluation / *Evaluation tasks* 10
4 La certification 11
4.1 Conclusion 11
4.2 Recommandations et limitations d'usage 12
4.3 Reconnaissance du certificat 12
4.3.1 Reconnaissance internationale critères communs (CCRA) 12
ANNEXE A. Références du PP / references for the protection profile 13
ANNEXE B. Références liées à la certification / Certification references 14

1 Résumé / *Summary*

Référence du rapport de certification / *Certification report reference*

EUCC-3090-2026-26

Nom du profil de protection / *Name of the protection profile*

Protection Profile PC Client Specific TPM

Référence/version du profil de protection / *Reference/version of the protection profile*

PP PCCS TPM F2.0 V2.0

Conformité à un profil de protection / *Conformity with a protection profile*

Néant / None

PP-Base certifiée / *Certified PP-Base*

Néant / None

PP-Modules associés aux PP-Configurations certifiées / *PP-Modules related to certified PP configurations*

Néant / None

Critère d'évaluation et version / *Evaluation criteria and version*

Critères Communs Version CC:2022

ISO/IEC 15408:2022 et ISO/IEC 18045:2022

Niveau d'évaluation imposé par le PP / *Evaluation level required by the PP*

Elevé / EAL 4 augmenté

ALC_FLR.2, ALC_DVS.2, AVA_VAN.4

Référence du rapport d'évaluation / *Evaluation report reference*

Evaluation Technical Report TCG TPM2.0 PP v2.0
référence TCG_TPM_PP_CC2022_ETR
version 1.0
28/01/2026

Rédacteur / *Author*

TRUSTED COMPUTING GROUP
3855 SW 153rd Drive,
Beaverton, OR 97003, USA

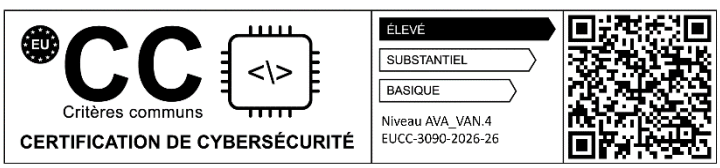
Commanditaire / *Sponsor*

TRUSTED COMPUTING GROUP
3855 SW 153rd Drive,
Beaverton, OR 97003, USA

Centre d'évaluation / *Evaluation facility (ITSEF)*

THALES / CNES
290 allée du Lac,
31670 Labège, France

Marque EUCC / *EUCC Mark*



Accords de reconnaissance applicables / *Applicable recognition agreements*

CCRA

2 Le profil de protection / *Protection profile*

2.1 Identification du profil de protection / *Identification of the protection profile*

Titre : *Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0*

Référence : PP PCCS TPM F2.0 V2.0

Date : 3 décembre 2025

2.2 Rédacteur / Author

Ce profil de protection a été rédigé par */ This protection profile has been writen by* :

TRUSTED COMPUTING GROUP

3855 SW 153rd Drive,

Beaverton, OR 97003,

Etats Unis d'Amérique

2.3 Description du profil de protection / *Description of the protection profile*

Le profil de protection a été rédigé par le groupe de travail responsable du cadre des évaluations sécuritaires du TRUSTED COMPUTING GROUP.

The protection profile was written by the TRUSTED COMPUTING GROUP work group responsible for security evaluation framework.

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.

The TRUSTED COMPUTING GROUP is a not-for-profit organization formed to develop, define, and promote open industry standards supportive of a hardware based root of trust for interoperable trusted computing platforms.

Le TPM, module de plateforme de confiance, est un composant électronique avec un logiciel embarqué. Il est destiné à être intégré dans des systèmes tels que des ordinateurs, serveurs ou du matériel de télécommunication qui implémentent les fonctionnalités définies par les spécifications de la librairie TPM 2.0 level 0 révision 1.59 ou 1.83.

The TPM, Trusted Platform Module, is an electronic component with embedded software. It is intended to be integrated into systems such as computers, servers or telecommunications equipment that implement the features defined by the TPM 2.0 library specifications, level 0 revision 1.59 or 1.83.

Le profil de protection comporte un package fonctionnel optionnel portant sur la fonctionnalité ECDAA des spécifications.

The protection profile includes an optional functional package covering the ECDAA functionality of the specifications.

2.4 Exigences fonctionnelles / functional requirements

Le profil de protection reprend les exigences fonctionnelles de sécurité suivantes définies dans les des Critères Communs [CC] / *the protection profile uses the following security functional requirements from the Common Criteria [CC]* :

- *Selected proof of origin* (FCO_NRO.1) ;
- *Cryptographic key generation* (FCS_CKM.1) ;
- *Timing and event of cryptographic key destruction* (FCS_CKM.6) ;
- *Cryptographic operation* (FCS_COP.1) ;
- *Generation of random numbers* (FCS_RNG.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).

2.5 Exigences d'assurance / Assurance requirements

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4 augmenté des composants d'assurance suivants ALC_FLR.2, ALC_DVS.2 et AVA_VAN.4**.

The protection profile requires for the TOE the assurance EAL4 augmented with ALC_FLR.2, ALC_DVS.2 and AVA_VAN.4.

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

All assurance components required by the protection profile are defined in Part 3 of the Common Criteria [CC].

La reconnaissance CCRA des produits évalués selon ce profil de protection sera limitée à EAL2 augmenté de ALC_FLR.2.

The CCRA recognition of a TOE whose security target conforms to this protection profile will be limited to EAL3 augmented with ALC_FLR.2.

2.6 Contacts du PP / *PP contacts*

Les informations en matière de cybersécurité du type de produit visé par ce profil de protection sont disponibles ici :

The PP's product type cybersecurity information is available here:

- https://trustedcomputinggroup.org/about/security/

Le rédacteur peut être contacté via cette adresse ou ce formulaire :

The author can be contacted at:

- admin@trustedcomputinggroup.org
- https://trustedcomputinggroup.org/about/contact

La procédure de signalement d'une vulnérabilité est disponible sur le lien suivant :

The complete procedure for reporting a vulnerability is available at the following link:

- https://trustedcomputinggroup.org/about/security/
- TCG PSIRT email : security@trustedcomputinggroup.org

Les informations sur l'autorité nationale de certification de cybersécurité en France sont disponibles ici :

Information on France's National Cybersecurity Certification Authority is available here:

- https://cyber.gouv.fr/cybersecurity-act .

3 L'évaluation / *Evaluation*

3.1 Référentiels d'évaluation / *Evaluation reference bases*

L'évaluation a été menée conformément aux Critères Communs Version 2022 [CC], à la méthodologie d'évaluation définie dans le manuel [CEM].

The evaluation was carried out in accordance with the Common Criteria [CC], and with the evaluation methodology defined in the manual [CEM].

3.2 Travaux d'évaluation / *Evaluation tasks*

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 janvier 2026, 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** ».

*The Evaluation Technical Report [ETR], submitted to ANSSI on January 28th, 2026, details the work carried out by the evaluation center and attests that all the evaluation tasks were rated as « **PASS** ».*

Les composants évalués (définis dans [CC]) sont les suivants :

The evaluated components (defined in [CC]) are:

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

4 La certification

4.1 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 et à [EUCC].

The evaluation was carried out according to current rules and standards, with the levels of competence and impartiality required for an approved evaluation body. All of the evaluation work performed permits the delivery of a certificate in accordance with decree 2002-535 and to [EUCC].

Le certificat associé à ce rapport, référencé EUCC-3090-2026-26, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de vingt ans à partir de cette date.

The certificate associated with this report, referenced EUCC-3090-2026-26 has an issue date identical to the signature date of this report and is valid for twenty years from that date.

Le certificat est délivré sous accréditation du COFRAC, attestation n°5-0669, portée disponible sur www.cofrac.fr.

The certificate is issued under COFRAC accreditation, number 5-0669, the scope can be found on www.cofrac.fr.

4.2 Recommandations et limitations d'usage

Aucune limitation d'usage ou recommandation particulière n'est à mentionner dans le présent rapport de certification.

There is no specific limit or guidance to report.

4.3 Reconnaissance du certificat

4.3.1 *Reconnaissance internationale critères communs (CCRA)*

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. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

The Common Criteria Recognition Arrangement (CCRA) allows signatory countries to recognize Common Criteria certificates. Recognition applies to APE insurance classes. Certificates recognized under this agreement are issued with the following mark:

[1] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références du PP / references for the protection profile

[PP]	*Protection Profile PC Client Specific TPM, TPM Library Specification Family* "2.0", version 2.0, 3 décembre 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report, TCG TPM2.0 PP* v2.0, TCG_TPM_PP_CC2022_ETR, version 1.0, 27 janvier 2026.

ANNEXE B. Références liées à la certification / Certification references

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. *Amended decree No. 2002-535 of April 18th, 2002 relating to the evaluation and certification of the security provided by information technology products and systems.*	
[CER-P-01]	Certification de cybersécurité fondé sur les critères communs pour les produits et les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4. *Cybersecurity Certification based on the Common Criteria for products and protection profiles, ref ANSSI-CC-CER-P-01.*
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, novembre 2022, version CC:2022, révision 1, référence CCMB-2022-11-001 ; - *Part 2 : Security functional components*, novembre 2022, version CC:2022, révision 1, référence CCMB-2022-11-002 ; - *Part 3 : Security assurance components*, novembre 2022, version CC:2022, révision 1, référence CCMB-2022-11-003 ; - *Part 4 : Framework for the specification of evaluation methods and activities*, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-004 ; - *Part 5 : Pre-defined packages of security requirements*, novembre 2022, version CC :2022, révision 1, référence CCMB-2022-11-005.
[ISO]	- *Part 1 : Introduction and general model*, août 2022, référence ISO/IEC 15408-1 ; - *Part 2 : Security functional components*, août 2022, référence ISO/IEC 15408-2 ; - *Part 3 : Security assurance components*, août 2022, référence ISO/IEC 15408-3 ; - Part 4 : Framework for the specification of evaluation methods and activities, août 2022, référence ISO/IEC 15408-4 ; - *Part 5 : Pre-defined packages of security requirements*, août 2022, référence ISO/IEC 15408-5.
[CC-Errata]	*Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)*, ref. 002, version 1.1, 22/07/2024.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, novembre 2022, version CEM :2022, révision 1, référence CCMB-2022-11-006.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements. *European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.*