
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-2019/02 du profil de protection « Automotive-Thin Specific TPM (Family "2.0") » Level 0 version 1.0

*Paris, le 4 juillet 2019*

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

[ORIGINAL SIGNE]

Guillaume POUPARD

# 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*<br>**ANSSI-CC-PP-2019/02** |
| *Nom du profil de protection*<br>**Automotive-Thin Specific TPM (Family "2.0")** |
| *Référence/version du profil de protection*<br>**PP AutoThin TPM F2.0 L0 V10/ Level 0 version1.0** |
| *Conformité à un profil de protection*<br>**Néant** |
| *PP-Base certifiée*<br>**Automotive-Thin Specific TPM** |
| *PP-Module associé aux PP-Configurations certifiées*<br>**Field Upgrade Module** |
| *Critères d'évaluation et version*<br>**Critères Communs version 3.1, révision 5** |
| *Niveau d'évaluation imposé par le PP*<br>**EAL 4 augmenté**<br>**ALC_FLR.1, AVA_VAN.4** |
| *Rédacteur(s)*<br>**Trusted Computing Group**<br>**3855 SW 153rd Drive**<br>**Beaverton, OR 97006, U.S.A** |
| *Commanditaire*<br>**Trusted Computing Group**<br>**3855 SW 153rd Drive**<br>**Beaverton, OR 97006, U.S.A** |
| *Centre d'évaluation*<br>**THALES / CNES**<br>**290 allée du Lac, 31670 Labège, France** |
| *Accords de reconnaissance applicables*<br>**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 : Automotive-Thin Specific TPM
Référence, version : PP AutoThin TPM F2.0 L0 V10, Level 0 version 1.0
Date : 12 décembre 2018

## 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 TPM[1] défini dans le profil de protection [PP] est destiné à être embarqué au sein d'un véhicule, et comprend un sous-ensemble des fonctionnalités définies dans la spécification TPM 2.0 et intégrées au profil de protection *PC Client Specific TPM* (précédemment certifié sous la référence [ANSSI-CC-PP-2018/03]) ainsi qu'une interface spécifique dédiée à son intégration dans un ECU[2].

Le PP comprend un profil de protection de base auquel peut s'ajouter un module optionnel, appelé *Field Upgrade Module*, correspondant à des fonctionnalités permettant la mise à jour du TPM en phase d'utilisation.

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. Les configurations évaluées sont définies dans le chapitre 1.6.

## 1.4. Exigences fonctionnelles

Une seule **exigence fonctionnelle de sécurité** est définie par le profil de protection[3] :

- FCS_RNG.1 Random numbers generation.

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

- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key destruction (FCS_CKM.4)

[1] *Trusted Platform Module*.
[2] *Electronic Control Unit.*
[3] Exigence fonctionnelle étendue non issue de la partie 2 des [CC].

- 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)
- Basic internal transfer protection (FDP_ITT.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring (FDP_SDI.1)
- Timing of identification (FIA_UID.1)
- Timing of authentication (FIA_UAU.1)
- Multiple authentication mechanisms (FIA_UAU.5)
- Re-authenticating (FIA_UAU.6)
- User-subject binding (FIA_USB.1)
- Authentication failure handling (FIA_AFL.1)
- TSF Generation of secrets (FIA_SOS.2)
- 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)
- Basic internal TSF data transfer protection (FPT_ITT.1)
- TSF testing (FPT_TST.1)
- Selective proof of origin (FCO_NRO.1)
- Inter-TSF trusted channel (FTP_ITC.1)
- Import of user data with security attributes (FDP_ITC.2)
- Export of user data with security attributes (FDP_ETC.2)
- Basic data exchange confidentiality (FDP_UCT.1)
- Data exchange integrity (FDP_UIT.1)
- Subset residual information protection (FDP_RIP.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 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].

## 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 « *Field Upgrade Module*».

# 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 25 juin 2019, 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** ».

L'évaluateur a appliqué les tâches APE à chacune des deux configurations résultant de la combinaison entre le profil de protection de base et le PP-module, comme s'il s'agissait de profils de protection standards, tel que prévu au chapitre 10.1 de [CEM] ; pour les deux configurations identifiées au chapitre 1.6, les composants évalués (définis dans [CC]) sont ainsi 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[1], 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 :


[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

## 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[1], 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 :

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

[1] 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 the 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** | |
| | ALC_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 | **4** | Production support, acceptance procedures and automation |
| | 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 flow 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** | **Methodical 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. | |
| [CPP-P-01] | Procédure ANSSI-CC-CPP-P-01 Certification de profils de protection, version 2 du 30 mai 2011. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;<br>- Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;<br>- 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 :<br>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. |
| [ANSSI-CC-PP-2018/03] | Rapport de certification ANSSI-CC-PP-2018/03 du profil de protection « PC Client Specific TPM » (TPM Library specification Family “2.0”, Level 0, Revision 1.38, Version 1.1), 10 août 2018. |
| [PP] | « Protection Profile Automotive-Thin Specific TPM », référence: PP AutoThin TPM F2.0 L0 V10, Level 0 version 1.0, 12 décembre 2018. |
| [RTE] | Evaluation Technical Report - Project: TPM Automotive-Thin Protection Profile, référence: TPMAT_ETR, version 2.0, 25 juin 2019. |