PREMIÈRE 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-2023/01

MCU Root of Trust Protection Profile (GPT_SPE_146, version 1.0)

Paris, le 10 Février 2023

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

Vincent STRUBEL

[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

Référence du rapport de certification **ANSSI-CC-PP-2023/01**
Nom du profil de protection **MCU Root of Trust Protection Profile**
Référence/version du profil de protection **GPT_SPE_146, version 1.0**
Conformité à un profil de protection Néant
PP-Base certifiée core PP MCU Root of Trust
PP-Modules associés aux PP-Configurations certifiées MCU RoT Persistent Time PP-Module, MCU RoT Debug PP-Module, MCU RoT ARoT Isolation PP-Module
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation imposé par le PP **EAL 2 augmenté** ALC_FLR.2, AVA_VAN_AP.3
Rédacteur **GLOBALPLATFORM, INC.** 544 Hillside Rd – *Redwood City*, CA 94062 – United States
Commanditaire **GLOBALPLATFORM, INC.** 544 Hillside Rd – *Redwood City*, CA 94062 – United States
Centre d'évaluation **THALES / CNES** 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables **CCRA** **SOG-IS**

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.

TABLE DES MATIERES

1 Le profil de protection

1.1 Identification du profil de protection

Titre : MCU Root of Trust Protection Profile

Référence, version : GPT_SPE_146, version 1.0

Date : décembre 2022.

1.2 Rédacteur

Ce profil de protection a été rédigé par :

GLOBALPLATFORM, INC.

544 Hillside Rd – Redwood City,

CA 94062 – United States

1.3 Description du profil de protection

Le profil de protection a été rédigé à partir du profil de protection *GlobalPlatform Trusted Execution Environment (TEE)* [PP TEE] dans le but d'être la référence pour l'évaluation des racines de confiance sur microcontrôleur dans les schémas de certification Critères Communs (CC) ou *GlobalPlatform*. Sa conception a été initiée par le groupe de travail *PSA JSA* puis finalisée par le comité *GlobalPlatform TEE*.

La cible d'évaluation *MCU RoT*, *Microcontroller Unit Root of Trust*, définie dans le profil de protection [PP], est un environnement d'exécution isolé implémenté sur microcontrôleur et ses sous-systèmes de confiance. En outre, il peut héberger des applications, nommées *Application Roots of Trust (ARoTs),* et leur offrir des services de sécurité incluant de la vérification d'intégrité de l'exécution, du stockage sécurisé, de la gestion de clés et d'algorithmes cryptographiques, de la gestion du temps et de l'attestation.

Le profil de protection *MCU Root of Trust* comprend un profil de protection de base appelé *core PP MCU RoT* auquel peuvent s'ajouter trois PP-Modules optionnels :

- *MCU RoT Persistent Time PP-Module* définit une fonctionnalité supplémentaire d'horloge monotone persistante entre chaque cycle de courant ;
- *MCU RoT Debug PP-Module* définit une interface de *debug* lors de la phase d'utilisation du produit pour les utilisateurs autorisés seulement ;
- *MCU RoT ARoT Isolation PP-Module* définit une fonctionnalité de sécurité supplémentaire fournissant un environnement d'exécution isolé pour les applications *ARoTs*.

Ce profil de protection autorise plusieurs configurations. Le profil de protection *core PP MCU RoT* peut être utilisé seul ou dans une PP-Configuration avec un sous-ensemble quelconque d'un, deux ou trois PP-Modules. Le profil de protection [PP] définit implicitement ces PP-Configurations qui sont listées dans la section 1.6.

1.4 Exigences fonctionnelles

Les **exigences fonctionnelles étendues de sécurité** définies par le profil de protection, au chapitre 6 du [PP], sont les suivantes :

- *Random numbers generation* (FCS_RNG.1)
- *TSF initialization* (FPT_INI.1)

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

- *Security alarms* (FAU_ARP.1) ;
- *Audit review* (FAU_SAR.1) ;
- *Protected audit trail storage* (FAU_STG.1) ;
- *Selective proof of origin* (FCO_NRO.1) ;
- *Cryptographic operation* (FCS_COP.1) ;
- *Subset access control* (FDP_ACC.1) ;
- *Security attribute based access control* (FDP_ACF.1) ;
- *Complete information flow control* (FDP_IFC.2) ;
- *Simple security attributes (*FDP_IFF.1) ;
- *Basic internal transfer protection* (FDP_ITT.1) ;
- *Subset residual information protection* (FDP_RIP.1) ;
- *Basic rollback* (FDP_ROL.1) ;
- *Stored data integrity monitoring and action* (FDP_SDI.2) ;
- *User attribute definition* (FIA_ATD.1) ;
- *User identification before any action* (FIA_UID.2) ;
- *User-subject binding* (FIA_USB.1) ;
- *Management of security attributes* (FMT_MSA.1) ;
- *Static attribute initialisation* (FMT_MSA.3) ;
- *Specification of management functions* (FMT_SMF.1) ;
- *Security roles* (FMT_SMR.1) ;
- *Failure with preservation of secure state* (FPT_FLS.1) ;
- *Basic internal TSF data transfer protection* (FTP_ITT.1) ;
- *Reliable time stamps* (FPT_STM.1) ;
- *Testing of external entities* (FPT_TEE.1).

1.5 Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL 2 augmenté des composants d'assurance suivants ALC_FLR.2 et AVA_VAN_AP.3**. AVA_VAN_AP.3 correspond à un une extension du composant d'assurance AVA_VAN.2 permettant à l'évaluateur d'avoir possiblement accès à des parties de la représentation de l'implémentation[1] et exigeant que les tests de pénétration soient effectués en considérant un attaquant de niveau *Enhanced-basic*.

En dehors du composant d'assurance étendu **AVA_VAN_AP.3**, toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

Les reconnaissances SOG-IS et CCRA des produits évalués selon ce profil de protection seront limitées à EAL 2 augmenté du composant ALC_FLR.2

[1] Au sens des [CC] : code source logicielle ou matériel, schéma de circuit, etc.

1.6 Configurations évaluées

Huit PP-Configurations ont été évaluées et sont certifiées :

1. Profil de protection (PP) de base *core PP MCU RoT* seul ;
2. PP de base *core PP MCU RoT* avec le PP-Module *MCU RoT Persistent Time* ;
3. PP de base *core PP MCU RoT* avec le PP-Module *MCU RoT Debug* ;
4. PP de base *core PP MCU RoT* avec le PP-Module *MCU RoT ARoT Isolation* ;
5. PP de base *core PP MCU RoT* avec les PP-Modules *MCU RoT Persistent Time* et *MCU RoT Debug* ;
6. PP de base *core PP MCU RoT* avec les PP-Modules *MCU RoT Debug* et *MCU RoT ARoT Isolation* ;
7. PP de base *core PP MCU RoT* avec les PP-Modules *MCU RoT Persistent Time* et *MCU RoT ARoT Isolation* ;
8. PP de base *core PP MCU RoT* avec les PP-Module *MCU RoT Persistent Time*, *MCU RoT Debug* et *MCU RoT ARoT Isolation*.

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 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 janvier 2023, 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 PP-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	*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 pour la configuration 1

Pour les PP-Configurations 2 à 8 (Profil de protection de base et les différents PP-Modules) les composants évalués sont les suivants :

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

Tableau 2 - Evaluation des PP-Configurations 2 à 8

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[2], 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[3], 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 :

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

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

ANNEXE A. Références

[PP]	*MCU Root of Trust Protection Profile*, référence GPT_SPE_146, version 1.0, décembre 2022, GLOBALPLATFORM INC.
[RTE]	Rapport technique d'évaluation : - *Protection Profile Evaluation Technical Report PP_MCU Root of Trust*, référence PP_MCU_APE, version 1.0, 2 janvier 2023.
[PP TEE]	*GlobalPlatform Technology Trusted Execution Environment Protection Profile*, référence GPD_SPE_021, version 1.3, GLOBALPLATFORM INC.

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 5.0.
[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.
[CCRA]	*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.