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-2022/01

Baseboard Management Controller Protection Profile with Firmware update Module (Version 1.0)

Paris, le 14 novembre 2022

Le Directeur général adjoint de l'Agence
nationale de sécurité des systèmes d'information

Emmanuel NAEGELEN

[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-2022/01**
Nom du profil de protection **Baseboard Management Controller Protection Profile with Firmware update module**
Référence/version du profil de protection **Version 1.0**
Conformité à un profil de protection Néant
PP-Base certifiée **Protection Profile for Baseboard Management Controller**
PP-Modules associés aux PP-Configurations certifiées **FWU PP-module for firmware update**
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation imposé par le PP **EAL 2 augmenté** ALC_FLR.1
Rédacteur **HUAWEI TECHNOLOGIES CO., LTD** 18 quai du Point du Jour 92659 Boulogne Billancourt, France
Commanditaire **HUAWEI TECHNOLOGIES CO., LTD** 18 quai du Point du Jour 92659 Boulogne Billancourt, France
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 : *Baseboard Management Controller Protection Profile with Firmware update module*

Référence, version : 1.0

Date : 28 septembre 2022

1.2 Rédacteur

Ce profil de protection a été rédigé par :

HUAWEI TECHNOLOGIES CO., LTD

18 quai du Point du Jour

92659 Boulogne Billancourt

France

1.3 Description du profil de protection

Le profil de protection a été rédigé par HUAWEI TECHNOLOGIES CO., LTD dans l'objectif d'homogénéiser les évaluations des contrôleurs de gestion de carte mère notamment le périmètre d'évaluation et les spécifications.

Le contrôleur de gestion de carte mère (*Baseboard Management Controller* – BMC) définit dans le profil de protection [PP] est un système informatique autonome permettant la gestion et la maintenance hors bande du serveur auquel il appartient.

Il est habituellement intégré à la carte mère du serveur et connecté au réseau dédié de gestion par une interface indépendante physique ou logique.

Le PP comprend un profil de protection de base auquel peut s'ajouter un PP-module optionnel :

- *FWU PP-module* : implémentation de la fonction de mise à jour sécurisée du *firmware*

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

Les **exigences fonctionnelles de sécurité** définies par le profil de protection[1] sont les suivantes :

- *Firmware Package Validation* (FPT_FPV.1) ;
- *Root of Trust based on HW* (FPT_HWROT.1) ;
- *Root of trust secure booting* (FPT_ROTSB.1) ;
- *Random Number Generation* (FCS_RNG.1) ;
- *FW Update – HW Support* (FPT_FWU.1).

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

- *Audit data generation* (FAU_GEN.1) ;

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

- *User identity association* (FAU_GEN.2) ;
- *Audit review* (FAU_SAR.1) ;
- *Restricted audit review* (FAU_SAR.2) ;
- *Protected audit trail storage* (FAU_STG.1) ;
- *Action in case of possible audit data loss* (FAU_STG.3) ;
- *Cryptographic key generation* (FCS_CKM.1) ;
- *Cryptographic key destruction* (FCS_CKM.4) ;
- *Cryptographic operation* (FCS_COP.1) ;
- *Authentication failure handling* (FIA_AFL.1) ;
- *Verification of secrets* (FIA_SOS.1) ;
- *User authentication before any action* (FIA_UAU.2) ;
- *Multiple authentication mechanisms* (FIA_UAU.5) ;
- *Protected authentication feedback* (FIA_UAU.7) ;
- *User identification before any action* (FIA_UID.2) ;
- *Management of security functions behaviour* (FMT_MOF.1) ;
- *Specification of management functions* (FMT_SMF.1) ;
- *Security roles* (FMT_SMR.1) ;
- *Failure with preservation of secure state* (FPT_FLS.1) ;
- *Automated recovery without undue loss* (FPT_RCV.3) ;
- *Reliable time stamps* (FPT_STM.1) ;
- *TSF testing* (FPT_TST.1) ;
- *TSF-initiated termination* (FTA_SSL.3) ;
- *Default TOE access banners* (FTA_TAB.1) ;
- *TOE session establishment* (FTA_TSE.1) ;
- *Inter-TSF trusted channel* (FTP_ITC.1) ;
- *Trusted path* (FTP_TRP.1).

1.5 Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL2 augmenté du composant d'assurance ALC_FLR.1**.

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

Les produits évalués selon ce profil de protection bénéficieront des reconnaissances SOG-IS et CCRA.

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 « *FWU PP-module* » .

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 4 octobre 2022, 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	*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 la configuration 2 (Profil de protection de base et le PP-module) les composants évalués (définis dans [CC]) 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 du PP pour la configuration 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[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]	*Baseboard Management Controller Protection Profile with Firmware update Module*, version 1.0, 28 septembre 2022.
[RTE]	Rapport technique d'évaluation : - *Protection Profile Evaluation Technical Report Project: PP BMC*, référence BMC_APE, version 2.4, 4 octobre 2022.

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.