PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance ANSSI-CC-2016/15-M01

TPM 2.0 Hardware version FB5C85D ou FB5C85E, Firmware version 1.3.0.1 ou 1.3.1.0

Certificat de référence : ANSSI-CC-2016/15

Paris, le 14 novembre 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Rapport de certification ANSSI-CC-2016/15, TPM2.0 Hardware version FB5C85D, Firmware version 1.3.0.1.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	NPCT6xx TPM2.0 Changes – Security Impact Analysis, version 1.1, 8 August 2016, Nuvoton.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 8th, 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.

2. Identification du produit maintenu

Le produit maintenu est produit « TPM 2.0 Hardware version FB5C85D ou FB5C85E, Firmware version 1.3.0.1 ou 1.3.1.0 » développé par la société *NUVOTON*.

Le produit « TPM 2.0 Hardware version FB5C85D, Firmware version 1.3.0.1 » (référence, version) a été initialement certifié sous la référence ANSSI-CC-2016/15 (référence [CER]).

La version maintenue du produit est identifiable par les éléments suivants (voir [GUIDES]) :

- la version matérielle est obtenue par la lecture du registre RID qui renvoie respectivement les données :
  - « 0x01 » qui identifie la version FB5C85D ;
  - « 0x10 » qui identifie la version FB5C85E ;
- la version logicielle est obtenue par la commande TPM_GetCapability qui, pour les tags TPM_PT_FIRMWARE_VERSION_1 et TPM_PT_FIRMWARE_VERSION_2 renvoie respectivement les données :
  - « 00.01.00.03 » et « 00.00.00.01 » qui identifient la version 1.3.0.1 ;
  - « 00.01.00.03 » et « 00.00.00.01 » qui identifient la version 1.3.0.1.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- pour ce qui concerne l'implémentation matérielle du produit :
  - retrait d'une résistance de *pull-up* de la broche de remise à zéro ;
  - modification de la phase de *wakeup* SPI (*Serial Peripheral Interface*) en mode *idle* (séquence d'activation de l'horloge) ;
  - changement de la valeur du registre RID, indiquant le changement de la version matérielle ;
- pour ce qui concerne l'implémentation logicielle du produit :
  - des erreurs fonctionnelles mineures ont été corrigées ;
  - des modifications mineures ont été apportées principalement dues à l'évolution des spécifications.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables, du produit évalué et sont applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	NPCT65x Trusted Platform Module Version 2.0 (TPM2.0), Revision 1.4, July 2016, Nuvoton Technology.	[R-M01]
	NPCT65x TPM 2.0 Programmer's Guide, Revision 1.1, July 2016, Nuvoton Technology.	[R-M01]
	NPCT6xx User Product Information, revision 4.4, July 2016, Nuvoton Technology.	[R-M01]
	NPCT6xx Board Design Guide, Revision 1.4, May 2015, Nuvoton Technology.	[CER]
	NPCT620/622/650/652 Reference Schematics, Revision 1.16, May 2015, Nuvoton Technology.	[CER]
	NPCT65xxxxA TPM2.0 Guidance Document, Revision 1.3, June 2016, Nuvoton Technology.	[CER]
[ST]	Cible de sécurité de référence pour l'évaluation : - TPM2.0 Security Target, référence : TPM2.0_ Nuvoton_ST_V1.03_Internal, Version 1.03, July 18 2016, Nuvoton Technology. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - TPM2.0 Security Target – lite, référence : TPM2.0_ST_Nuvoton_V1.03_External, Version 1.03, July 18 2016, Nuvoton Technology.	[R-M01]
[CONF]	Liste de configuration du produit : - TPM2.0_NPCT6xx_IC_ALC_CMS, (HW FB5C85E with FW version 1.3.0.1), version 0.6.1, November 2015, Nuvoton Technology ; - TPM2.0_NPCT6xx_IC_ALC_CMS,version 0.6.2, November 2015, Nuvoton Technology ; - TPM2.0_NPCT6xx_IC_ALC_CMS,version 0.6.3, November 2015, Nuvoton Technology ; - ALC_Doc_Report TPM2.0, version 3.5, Nuvoton Technology.	[R-M01]

5. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur.**
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, à la date de certification.
Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

6. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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 les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été 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[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.