Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2015/14-M04

TPM 1.2 Hardware versions FB5C85D ou FB5C85E, Firmware versions 5.81.0.0, 5.81.1.0 ou 5.81.2.1

Certificat de référence : ANSSI-CC-2015/14

Paris, le 13 février 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2015/14, TPM1.2 Hardware version FB5C85D, Firmware version 5.81.0.0.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2015/14-M01, TPM1.2 Hardware version FB5C85E, Firmware version 5.81.0.0.
[R-M02]	Rapport de maintenance ANSSI-CC-2015/14-M02, TPM1.2 Hardware version FB5C85D ou FB5C85E, Firmware version 5.81.1.0.
[R-M03]	Rapport de maintenance ANSSI-CC-2015/14-M03, TPM1.2 Hardware version FB5C85D ou FB5C85E, Firmware version 5.81.2.1.
[IAR]	TPM1.2 Changes – Security Impact Analysis, ref. NPCT6xx_TPM1.2_M04_SIA, v.1.0, 30 October 2016, Nuvoton.
[RM-Lab]	Evaluation Technical Report Addendum, TPM2.0 and TPM1.2bis, ref. TPM_ETR_ADD_v1.0, 24/01/2017, Serma Safety and Security.
[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 le « TPM 1.2 », Hardware versions FB5C85D ou FB5C85E, Firmware versions 5.81.0.0, 5.81.1.0 ou 5.81.2.1 développé par la société *NUVOTON*.
Le produit « TPM 1.2 », Hardware version FB5C85D, Firmware version 5.81.0.0 a été initialement certifié sous la référence ANSSI-CC-2015/14 (référence [CER]). Il a déjà fait l'objet de trois maintenances sous les références ANSSI-CC-2015/14-M01 (référence [R-M01]), ANSSI-CC-2015/14-M02 (référence [R-M02]) et ANSSI-CC-2015/14-M03 (référence [R-M03]).
La version maintenue du produit est identifiable par les éléments suivants (voir [GUIDES]) :

- la version matérielle (FB5C85D/FB5C85E) est obtenue par la lecture du registre RID ;
- la version logicielle est obtenue par la commande TPM_GetCapability qui renvoie les données « 00.30.01.02.**05**.**51**.00.02.03.57.45.43.00.00.02.**02.01** », « 00.30.01.02.**05**.**51**.00.02.03.57.45.43.00.00.02.**00.00** » ou « 00.30.01.02.**05**.**51**.00.02.03.57.45.43.00.00.02.**01.00** » où les valeurs des octets en gras référencent respectivement les versions 5.81.0.0, 5.81.1.0 et 5.81.2.1.

3. Description des évolutions

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

- ajout dans le cycle de vie du site de fabrication de *wafer* suivant : *TOWERJAZZ PANASONIC* Semiconductor Corporation (TPSCo) - 271 Higashi-kaihotsu, Tonami City, Toyama, 939-1312, Japan ;

- ajout dans le cycle de vie du site de *wafer scrap* suivant : *MATSUDA SANGYO* Co. LTD, 87-1 Negishi, Iruma city, Saitama, 358-0034, Japan ;
- retrait du cycle de vie du site de fabrication de masques suivant : *TOPPAN PHOTOMASK*, 224 Boulevard Kennedy, 91105 Corbeil-Essonnes Cedex, France.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

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-M04] référence la présente maintenance.

[GUIDES]	Guide d'installation du produit : - NPCT6xx TPM Initialization and Configuration Application Note, June 2014, Nuvoton Technology.	[CER]
	Guides d'administration du produit : - NPCT62x LPC/SPI/I2C Trusted Platform Module (TPM) datasheet version 1.1, January 2016, Nuvoton Technology ; - NPCT62x/NPCT65x TPM1.2 with LPC, SPI and I2C Interfaces programmer's Guide, version 1.2, August 2015, Nuvoton Technology.	[R-M03] [R-M02]
	Guide d'utilisation du produit : - ARSUF (NPCT6xynA0 TPM 1.2) Operational Guidance Document, version 1.0, 3rd July 2014, Nuvoton Technology ; - NPCT6xx User Product Information, revision 4.1, December 2015.	[CER] [R-M03]
[ST]	Cibles de sécurité de référence: - TPM1.2bis Security Target, référence : TPM1.2bis_ST_Nuvoton_V0.73, 26 October 2016, Nuvoton Technology. Version publique : - TPM1.2bis Security Target - lite, référence : TPM1.2bis_ST_Nuvoton_V1.9_lite, 26 October 2016, Nuvoton Technology.	[R-M04] [R-M04]
[CONF]	- Arsuf IC_ALC_CMS.1 ,version 0.5.4 Nuvoton Technology (HW FB5C85D with FW 5.81.2.1) , 14 Feb. 2016, Nuvoton Technology ; - Arsuf IC_ALC_CMS.1 ,version 0.5.5 Nuvoton Technology (HW FB5C85E with FW 5.81.2.1), 14 Feb. 2016, Nuvoton Technology ; - ALC_Doc_Report, version1.5, Nuvoton Technology.	[R-M03] [R-M03] [R-M03]

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.

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.