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-M01

TPM 1.2 Hardware version FB5C85E, Firmware version 5.81.0.0

Certificat de référence : ANSSI-CC-2015/14

Paris, le 9 février 2016

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.
[IAR]	TPM1.2 Changes – Security Impact Analysis, version 2.1, 5 janvier 2016.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, Juillet 2014.

2. Identification du produit maintenu

Le produit maintenu est le « TPM 1.2 », Hardware version FB5C85E, Firmware version 5.81.0.0 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]).

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

- la version matérielle (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.**00.00** » où les octets « **05 51** » et « **00 00** » référencent la version 5.81.0.0.

Le boitier intégrant la TOE est identifié par les marquages externes suivants (dénomination commerciale courante) :

NPCT620AB0WX	NPCT620BA0WX	NPCT620CB0WX	NPCT620DB0WX
NPCT620HB0WX	NPCT620IB0WX	NPCT620LB0WX	NPCT620MB0WX
NPCT620NB0WX	NPCT620RB0WX	NPCT620SB0WX	NPCT620TB0WX
NPCT620UB0WX	NPCT620VB0WX	NPCT620JB0WX	NPCT620JB1WX
NPCT622AB0WX	NPCT622BB0WX	NPCT622CB0WX	NPCT622DB0WX
NPCT622HB0WX	NPCT622IB0WX	NPCT622LB0WX	NPCT622MB0WX
NPCT622NB0WX	NPCT622RB0WX	NPCT622SB0WX	NPCT622TB0WX
NPCT622UB0WX	NPCT622VB0WX	NPCT622JB0WX	NPCT620AB0YX
NPCT620BB0YX	NPCT620CB0YX	NPCT620DB0YX	NPCT620HB0YX
NPCT620IB0YX	NPCT620LB0YX	NPCT620MB0YX	NPCT620NB0YX
NPCT620RB0YX	NPCT620SB0YX	NPCT620TB0YX	NPCT620UB0YX
NPCT620VB0YX	NPCT620JB0YX	NPCT620JB1YX	NPCT622AB0YX
NPCT622BB0YX	NPCT622CB0YX	NPCT622DB0YX	NPCT622HB0YX
NPCT622IB0YX	NPCT622LB0YX	NPCT622MB0YX	NPCT622NB0YX
NPCT622RB0YX	NPCT622SB0YX	NPCT622TB0YX	NPCT622UB0YX
NPCT622VB0YX	NPCT622JB0YX	NPCT650AB0WX	NPCT650BB0WX
NPCT650CB0WX	NPCT650DB0WX	NPCT650HB0WX	NPCT650IB0WX

NPCT650LB0WX	NPCT650MB0WX	NPCT650NB0WX	NPCT650RB0WX
NPCT650SB0WX	NPCT650TB0WX	NPCT650UB0WX	NPCT650VB0WX
NPCT650JB0WX	NPCT652AB0WX	NPCT652BB0WX	NPCT652CB0WX
NPCT652DB0WX	NPCT652HB0WX	NPCT652IB0WX	NPCT652LB0WX
NPCT652MB0WX	NPCT652NB0WX	NPCT652RB0WX	NPCT652SB0WX
NPCT652TB0WX	NPCT652UB0WX	NPCT652VB0WX	NPCT652JB0WX
NPCT650AB0YX	NPCT650BB0YX	NPCT650CB0YX	NPCT650DB0YX
NPCT650HB0YX	NPCT650IB0YX	NPCT650LB0YX	NPCT650MB0YX
NPCT650NB0YX	NPCT650RB0YX	NPCT650SB0YX	NPCT650TB0YX
NPCT650UB0YX	NPCT650VB0YX	NPCT650JB0YX	NPCT652AB0YX
NPCT652BB0YX	NPCT652CB0YX	NPCT652DB0YX	NPCT652HB0YX
NPCT652IB0YX	NPCT652LB0YX	NPCT652MB0YX	NPCT652NB0YX
NPCT652RB0YX	NPCT652SB0YX	NPCT652TB0YX	NPCT652UB0YX
NPCT652VB0YX	NPCT652JB0YX		

3. Description des évolutions

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

- 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.

D'autre part, le périmètre du site de production suivant a été élargi par rapport au cycle de vie initial du produit pour le test final (voir le rapport d'audit de site [SITE]) :

- ASE 550, Chung-Hwa Road Section I, Chung-Li, 32016 TAIWAN.

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]	Guide d'installation du produit : - NPCT6xx TPM Initialization and Configuration Application Note, June 2014, Nuvoton Technology.	[CER]
	Guides d'administration du produit : - NPCT6xx LPC/SPI/I2C Trusted Platform Module (TPM) datasheet, version 0.94, April 2015, Nuvoton Technology ; - NPCT62x/NPCT65x TPM1.2 with LPC, SPI and I2C Interfaces programmer's Guide, version 1.1, April 2015, Nuvoton Technology.	[R-M01] [R-M01]
	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 4.0, October 2015, Nuvoton Technology.	[CER] [R-M01]
[ST]	Cibles de sécurité de référence: - TPM1.2bis Security Target, référence : TPM1.2bis_ST_Nuvoton_V0.7, 10 January 2016, Nuvoton Technology. Version publique : - TPM1.2bis Security Target - lite, référence: TPM1.2bis_ST_Nuvoton_V1.6_lite, 10 January 2016, Nuvoton Technology.	[R-M01] [R-M01]
[CONF]	- Arsuf IC_ALC_CMS.1 ,version 0.5, (HW FB5C85E with FW 5.81.1.0), Nuvoton Technology ; - ALC_Doc_Report, version 1.2, Nuvoton Technology.	[R-M01] [R-M01]
[SITE]	Rapport d'audit de site : - ASE Chung-Li Site Visit Report, référence C14P0082_ASE_SVR_v1.0, 21 October 2015, Serma Technologies.	[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 EAL4 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, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.