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-2017/75-M01

NPCT7xx TPM 2.0 Hardware version LAG019, Firmware version 7.2.0.2

Certificat de référence : ANSSI-CC-2017/75

Paris, le 18/04/2018

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-2017/758, « NPCT7xx TPM 2.0 Hardware version LAG019, Firmware version 7.2.0.1 », 19/1/2018, ANSSI.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	NPCT7xx TPM2.0 Changes Security Impact Analysis, version 1.6, 27/12/2018, *NUVOTON TECHNOLOGY ISRAEL LTD.* Voir §9 « Firmware Changes Description in version 2.0.0.59 compared to 2.0.0.54 ».
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CCRA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

2. Identification du produit maintenu

Le produit « NPCT7xx TPM 2.0, Hardware version LAG019, Firmware version 7.2.0.1 » développé par *NUVOTON TECHNOLOGY ISRAEL LTD*, a été initialement certifié sous la référence ANSSI-CC-2017/75 (référence [CER]).

Le produit objet de la présente maintenance est « NPCT7xx TPM 2.0, Hardware version LAG019, Firmware version 7.2.0.2 ».

La version maintenue du produit est identifiable par les éléments suivants (voir [ST] Section 1.1 – *Security Target (ST) and Target of Evaluation (TOE) Identification*) :

Register/Field	Value	Comments
TPM_DID_VID_x.VID (SPI), TPM_CRB_INTF_ID_x.VID (SPI), TPM_DID_VID.VID (I2C)	VID = 1050h DID = 00FCh	PTP Specification, Section 5.4.1.1 DID/VID Register. Offset: xF00h FIFO Register Space. PTP Specification, Section 5.4.2.2 CRB Interface Identifier Register. Offset: x030h CRB Register Space. PTP Specification, Section 7.3.5.13 TPM_DID_VID. Offset: 48h I2C Register Space.
TPM_RID_x (SPI), TPM_CRB_INTF_ID_x.RID (SPI), TPM_RID (I2C)	01h	PTP Specification, Section 5.4.1.2 RID Register. Offset: xF04h FIFO Register Space. PTP Specification, Section 5.4.2.2 CRB Interface Identifier Register. Offset: x030h CRB Register Space. PTP Specification, Section 7.3.5.14 TPM_RID. Offset: 4Ch I2C Register Space.
TPM_PT_MANUFACTURER	"NTC" = 4E544300h	TPM 2.0 Specification, Part 2, Section 6.13 TPM_PT (Property Tag)
TPM_PT_VENDOR_STRING_1	"NPCT" = 4E504354h	
TPM_PT_VENDOR_STRING_2	"75x" = 37357800h	
TPM_PT_VENDOR_STRING_3	02000036h	
TPM_PT_VENDOR_STRING_4	"rls" = 726C7300h	
Firmware version 7.2.0.2 TPM_PT_FIRMWARE_VERSION_1	**00070002h**	
TPM_PT_FIRMWARE_VERSION_2	**00000002h**	

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR] §9) mentionne que les modifications suivantes ont été opérées :

- corrections logicielles fonctionnelles dans le code du *firmware* ;
- incrément du numéro de version du *firmware* en conséquence.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides 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]	NPCT75x Programmer's Guide, version 1.1, mai 2018, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[R-M01]
	NPCT75x Trusted Platform Module Family 2.0, version 1.7, février 2019, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[R-M01]
	NPCT75x User product Information, version 2.2, janvier 2019, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[R-M01]
	NPCT75xxAC TPM2.0 Guidance document, version 1.1, 4/2/2019, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[R-M01]
	NPCT7xx_System_Setup_v1.0, version 1.0, 20/10/2016, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[CER]
[ST]	NPCT7xx TPM2.0 Public Security Target, version 1.01, 4/2/2019, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[R-M01]
[CONF]	NPCT7xx_TPM2.0_rev1.16_FW_7.2.0.2_IC_ALC_CMS.1.v1.0.0, version 1.0.0, 31/1/2019, *NUVOTON TECHNOLOGY ISRAEL LTD*.	[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.

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 cette 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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. 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 CCRA [CCRA].

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 :

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

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