



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 certification ANSSI-CC-2019/30

NPCT7xx TPM1.2 rev 116
Hardware version LAG019
Firmware version 7.4.0.0

Paris, le 14 août 2019

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

Emmanuel GERMAIN
[ORIGINAL SIGNE]



Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.



La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CC-2019/30
Nom du produit	NPCT7xx TPM1.2 rev 116
Référence/version du produit	Hardware LAG019, Firmware 7.4.0.0
Conformité à un profil de protection	PC Client Specific Trusted Platform Module, TPM Family 1.2, Level 2, Revision 116, version 1.3
Critères d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL 4 augmenté ALC.FLR.1, ALC_DVS.2, AVA_VAN.4
Développeur	Nuvoton Technology Israel Ltd. 8 Hasadnaot ST., P.O.B. 3007, Herzlia B, 46130 Israel
Commanditaire	Nuvoton Technology Israel Ltd. 8 Hasadnaot ST., P.O.B. 3007, Herzlia B, 46130 Israel
Centre d'évaluation	Serma Safety & Security 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
Accords de reconnaissance applicables	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div> <p>Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.</p>

Préface

La certification

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 Premier ministre 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 matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	7
1.2.5. <i>Cycle de vie</i>	8
1.2.6. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION	10
2.2. TRAVAUX D’EVALUATION	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	10
2.4. ANALYSE DU GENERATEUR D’ALEAS	10
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE	11
3.3. RECONNAISSANCE DU CERTIFICAT	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	12
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. RÉFÉRENCES LIÉES À LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est le *Trusted Platform Module* : « NPCT7xx TPM1.2 rev 116, Hardware LAG019, Firmware 7.4.0.0 » développé par *NUVOTON TECHNOLOGY ISRAEL LTD.*

Ce produit est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs, etc...) conformément aux spécifications fonctionnelles TPM¹ 1.2.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP-TPM].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'accès aux fonctions cryptographiques (RSA, AES, SHA1, SHA-256, HMAC) ;
- la séquence de démarrage et l'auto-test ;
- les fonctions de contrôle d'accès ;
- la protection physique par un bouclier actif (*active shield*) ;
- un ensemble de détecteurs de sécurité (*glitch*, parité, etc.) ;
- la génération de clés et le stockage des clés ;
- la génération de nombres aléatoires ;
- l'identification de la configuration ;
- l'authentification de l'entité propriétaire ;
- la mise à jour du logiciel embarqué dans le produit.

1.2.3. Architecture

Le produit est constitué principalement :

- d'une unité centrale ;
- des unités d'interfaces GPIO et SPI ;
- d'un générateur de nombres aléatoires ;
- des modules d'accélération cryptographique pour le support des calculs RSA, AES, SHA-1/SHA-256 ;
- des blocs mémoires de type ROM, RAM et Flash ;
- d'un *timer* sécurisé.

Cette architecture est résumée sur la figure suivante.

¹ *Trusted Platform Module.*

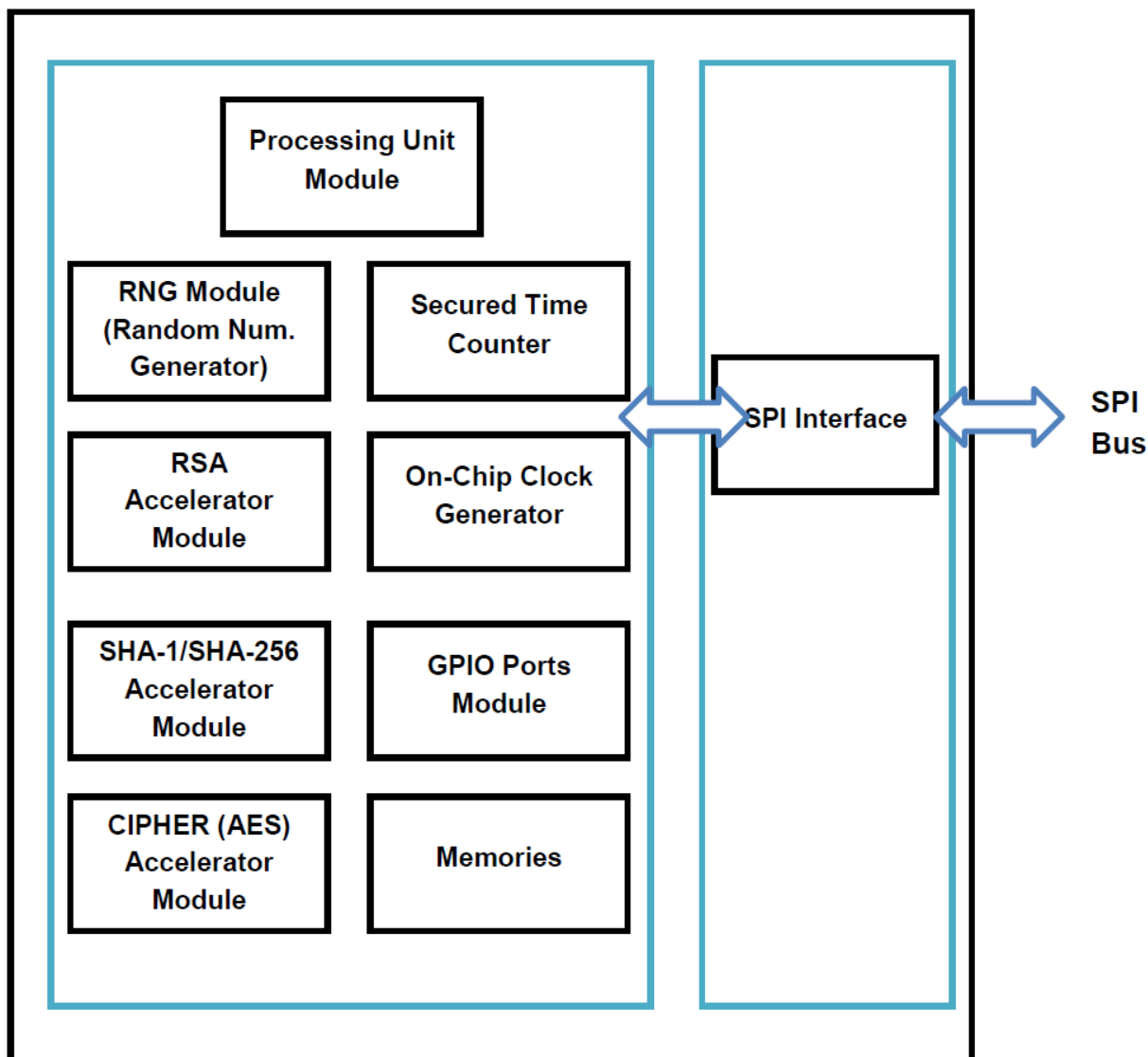


Figure 1. Architecture

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments suivants :

- la version matérielle « LAG019 » est identifiée par les registres (voir [GUIDES]) :
 - o VID = 0x1050 ;
 - o DID = 0x00FC ;
 - o RID = 0x01,
- la version logicielle est obtenue à l'aide de la commande « TPM_GetCapability » qui retourne les données identifiant la version *firmware* 7.4.0.0 (voir [GUIDES]). La version logicielle est associée aux données suivantes :
 - o version : {01h, 02h, 07h, 04h} (version de TPM 1.2, versions de *firmware* majeure 7 et mineure 4) ;
 - o niveau de spécification : 0002h (TPM family 1.2) ;
 - o version d'errata de la spécification : 03h (révision 116) ;
 - o identification du vendeur : 4E544300h (NTC pour Nuvoton Technology Corporation)

- version spécifique au vendeur : 0000h (0.0).
- La version *firmware* est donc bien identifiée 7.4.0.0.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]) qui est conforme à celui décrit dans le profil de protection (voir [PP-TPM]) et se décline en sept phases. Les classes d'assurance ALC couvrent les phases 1 (développement du TPM) et 2 (fabrication et livraison du TPM), alors que les phases 3 à 7 sont, elles, couvertes par les guides [GUIDES]. Pour les phases 3 à 7, après la livraison du produit, une fonctionnalité de mise à jour du *firmware* est disponible. Cette fonctionnalité possède un mécanisme de vérification de l'authenticité des données et seule une mise à jour provenant de *NUVOTON TECHNOLOGY ISRAEL LTD* est acceptée.

Le produit a été développé, fabriqué et expédié sur les sites certifiés décrits par la figure 2. Les rapports d'évaluations de sites effectuées dans le schéma français sont cités dans [SITES]. L'évaluation couvre la configuration finale du produit, c'est-à-dire celle obtenue en phase 7.

Design Center	
Design Center 1: Nuvoton Technology Israel Ltd.	Hasadnaot 8, Hertzlia, Israel
Design Center 2: Nuvoton Technology Israel Ltd	Ataa'sia 8, Ramat Gavriel, Migdal Haemek, Israel
Mask Fab	
TSMC Fab 14A	1-1, Nan-Ke North Rd., Tainan Science Park, Tainan 741-44, Taiwan, R.O.C.
Wafer Fab	
TSMC Fab 14A (mask and wafer manufacturing)	1-1, Nan-Ke North Rd., Tainan Science Park, Tainan 741-44, Taiwan, R.O.C.
TSMC Fab 8 (data center)	25, Li-Hsin Rd., Hsinchu Science Park, Hsinchu 300-78, Taiwan, R.O.C.
TSMC Fab 3 (eFlash IP merge)	9, Creation Rd. 1, Hsinchu Science Park, Hsinchu 300-77, Taiwan, R.O.C.
TSMC Fab 2 and 5 (mask data preparation)	121, Park Ave. 3, Hsinchu Science Park, Hsinchu 300-77, Taiwan, R.O.C.
Assembly Plants	
ASE Group Chung-Li	550, Chung-Hwa Road Section 1, Chung-Li, 320, Taiwan, R.O.C
UTL (UTAC Thailand 1 / QFN)	237 Lasalle Road, Bangna, Bangkok, 10260, Thailand
UTL (UTAC Thailand 2 / TSSOP)	78/1 Moo5, Bangsamak, Bangpakong, Chachoengsao, 24180, Thailand
Wafer Test & Final Test Plants	
Nuvoton Technology Corporation	No. 4, Creation Rd. III, Hsinchu Science Park, 300 Taiwan, R.O.C.
ASE Group Chung-Li	550, Chung-Hwa Road Section 1, Chung-Li, 320, Taiwan, R.O.C

Figure 2. Sites de développement et production du produit



1.2.6. Configuration évaluée

Le certificat porte sur le composant programmé avec l'application TPM 1.2, tel que présenté à la configuration décrite à la section « 1.2.3 Architecture » et configuré conformément au guide de personnalisation [GUIDES]. Le composant a été testé en mode opérationnel, mode dans lequel il est livré à l'utilisateur.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation des produits « NPCT7xx TPM2.0 » et « NPCT7xx TPM2.0 rev1.38 » certifiés respectivement les 19 janvier 2018 et 18 janvier 2019 sous les références respectives ANSSI-CC-2017/75 (voir [CER-2017]) et ANSSI-CC-2018/61 (voir [CER-2018]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 juin 2019, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.4 visé.

2.4. Analyse du générateur d'aléas

Comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.4 visé.



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.

Ce certificat atteste que le produit « NPCT7xx TPM1.2 rev 116, Hardware LAG019, Firmware 7.4.0.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2, ALC_FLR.1 et AVA_VAN.4.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- la taille minimale des clés RSA doit être d'au moins 2048 bits ;
- la fonction de *hash* SHA-1 ne doit pas être utilisée pour des applications de sécurité.

3.3. Reconnaissance du certificat

3.3.1. 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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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 La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR								1	1	Basic Flaw remediation
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	4	4	Moderate vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - NPCT7xx TPM1.2 rev 116 Security Target, référence NPCT7xx_TPM1.2_rev116_ST_Internal, version 1.0.5, datée du 4 avril 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD.</i> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - NPCT7xx TPM1.2 rev 116 Security Target, référence NPCT7xx_TPM1.2_rev116_ST_External, version 1.0.5, datée du 4 avril 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD.</i>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report – NPCT7_xx TPM1.2 rev 116 project, référence NPCT7_TPM1.2_ETR_v1.1, version 1.1, daté du 17 juin 2019, <i>SERMA SAFETY & SECURITY.</i>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - CM scope, référence NPCT7xx_TPM1.2_rev116_FW_7.4.0.0_IC_ALC_CMS.1, version 1.0.1, daté du 4 avril 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD ;</i> - CC Document Report, référence NPCT7xx_TPM1.2_rev116_Doc_Report, version 2.1, daté du 4 avril 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD ;</i> - NPCT7xx_Issues_DB_Snapshot, version 1.0, daté du 31 janvier 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD.</i>
[GUIDES]	<ul style="list-style-type: none"> - NPCT75xxA1 (NPCT75x Preloaded with TPM1.2) Operational Guidance Document Common Criteria AGD Component, référence NPCT75x_Guidance_TPM_1_2, version 1.2, daté du 6 février 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD ;</i> - NPCT75x Trusted Platform Module Version 1.2, référence NPCT75x_TPM1.2_DS, version 1.5, daté de juillet 2018, <i>NUVOTON TECHNOLOGY ISRAEL LTD ;</i> - NPCT7xx TPM1.2 User Product Information, référence NPCT75x_TPM1.2_Errata_Rev1.0, version 1.0, daté de janvier 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD ;</i> - NPCT75x TPM 1.2 Programmer's Guide, référence NPCT75x_TPM1.2_ProgGuide, version 1.2, daté de février 2019, <i>NUVOTON TECHNOLOGY ISRAEL LTD.</i>



[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - NUVOTON Development Environment (Generic Documentary activities – Full Report), référence Site_NUVOTON_2018_ALC_GEN_v1.1, daté du 20 juillet 2018, <i>SERMA SAFETY & SECURITY</i> ; - Site Technical Audit Report – NTC, Site_Nuvoton_2018_NTC_STAR_v1.1, version 1.1, daté du 19 juin 2019, <i>SERMA SAFETY & SECURITY</i> ; - Nuvoton development Environment NTIL STAR, référence NTIL_STAR_v1.2, version 1.2, daté du 19 juin 2019, <i>SERMA SAFETY & SECURITY</i> ; - Site Technical Audit Report – TSMC Fab 3, référence Site_NUVOTON_2019_STAR_v1.0, version 1.0, daté du 14 mai 2019, <i>SERMA SAFETY & SECURITY</i> ; - Site Technical Audit Report – Site_ATHENA2 Site Certification, référence Site_ATHENA_2_STAR_v1.1, version 1.1, daté du 7 mai 2019, <i>SERMA SAFETY & SECURITY</i> ; - Site Technical Audit Report – UTAC Thai Limited 1, référence UTL1.2_STAR_v1.0, version 1.0, daté du 6 décembre 2018, <i>SERMA SAFETY & SECURITY</i> ; - Site Technical Audit Report – UTL2.2 Site certification, référence UTL2.2_STAR_v1.0, version 1.0, daté du 6 décembre 2018, <i>SERMA SAFETY & SECURITY</i>.
[CER-2017]	<p>Rapport de certification ANSSI-CC-2017/75 – NPCT7xx TPM 2.0, Hardware version LAG019, Firmware version 7.2.0.1. <i>Certifié par l'ANSSI le 19 janvier 2018 sous la référence ANSSI-CC-2017/75.</i></p>
[CER-2018]	<p>Rapport de certification ANSSI-CC-2018/61 – NPCT7xx TPM 2.0 rev1.38, Hardware version LAG019, Firmware version 7.2.1.0. <i>Certifié par l'ANSSI le 18 janvier 2019 sous la référence ANSSI-CC-2018/61.</i></p>
[PP-TPM]	<p>Protection Profile - PC Client Specific Trusted Platform Module, TPM Family 1.2, level 2, revision 116, version 1.3. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 27 août 2008 sous la référence BSI-CC-PP-0030-2008 et maintenu le 18/12/2014 sous la référence BSI-CC-PP-0030-2008-MA-02.</i></p>

Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure ANSSI-CC-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, ANSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation :</p> <ul style="list-style-type: none"> - 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]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.</p>
[JIWG IC] *	<p>Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.</p>
[JIWG AP] *	<p>Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.</p>
[SOG-IS]	<p>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</p>
[REF]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.</p>
	<p>Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.</p>
	<p>Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.</p>

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.