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-2015/14

TPM 1.2

Hardware version FB5C85D, Firmware version 5.81.0.0

Paris, le 13 mai 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 présupposées 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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2015/14

Nom du produit

TPM 1.2

Référence/version du produit

Hardware version FB5C85D, Firmware version 5.81.0.0

Conformité à un profil de protection

[BSI-CC-PP-0030-2008-MA-01], version v1.2
PC Client Specific Trusted Platform Module TPM, Family 1.2

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, ALC_FLR.1, AVA_VAN.4

Développeur

Nuvoton Technology Israel Ltd.

8 Hasadnaot St, POB 3007, Herzlia B. 46130, Israël

Commanditaire

Nuvoton Technology Israel Ltd.

8 Hasadnaot St, POB 3007, Herzlia B. 46130, Israël

Centre d'évaluation

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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

1.1. Présentation du produit

Le produit évalué est le composant « TPM 1.2, Hardware version FB5C85D, Firmware version 5.81.0.0 » développé par *NUVOTON TECHNOLOGY ISRAEL LTD*.

Ce produit est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs…) conformément aux spécifications fonctionnelles TPM (*Trusted Platform Module*).

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.

La cible de sécurité est conforme au profil de protection [BSI-CC-PP-0030-2008-MA-01].

1.2.2. Identification du produit

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

La version certifiée de la TOE est identifiable par les éléments suivants (voir [GUIDES]) :

- la version matérielle « FB5C85 » est inscrite sur le composant ;
- 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 valeurs « 05 51 » référencient la version 5.81.0.0.

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

NPCT620AA0WX	NPCT620BA0WX	NPCT620CA0WX	NPCT620DA0WX
NPCT620HA0WX	NPCT620IA0WX	NPCT620LA0WX	NPCT620MA0WX
NPCT620NA0WX	NPCT620RA0WX	NPCT620SA0WX	NPCT620TA0WX
NPCT620UA0WX	NPCT620VA0WX	NPCT620JA0WX	NPCT620JA1WX
NPCT622AA0WX	NPCT622BA0WX	NPCT622CA0WX	NPCT622DA0WX
NPCT622HA0WX	NPCT622IA0WX	NPCT622LA0WX	NPCT622MA0WX
NPCT622NA0WX	NPCT622RA0WX	NPCT622SA0WX	NPCT622TA0WX
NPCT622UA0WX	NPCT622VA0WX	NPCT622JA0WX	NPCT620AA0YX
NPCT620BA0YX	NPCT620CA0YX	NPCT620DA0YX	NPCT620HA0YX
NPCT620IA0YX	NPCT620LA0YX	NPCT620MA0YX	NPCT620NA0YX
NPCT620RA0YX	NPCT620SA0YX	NPCT620TA0YX	NPCT620UA0YX
NPCT620VA0YX	NPCT620JA0YX	NPCT620JA1YX	NPCT622AA0YX
NPCT622BA0YX	NPCT622CA0YX	NPCT622DA0YX	NPCT622HA0YX
NPCT622IA0YX	NPCT622LA0YX	NPCT622MA0YX	NPCT622NA0YX
NPCT622RA0YX	NPCT622SA0YX	NPCT622TA0YX	NPCT622UA0YX

NPCT622VA0YX	NPCT622JA0YX	NPCT650AA0WX	NPCT650BA0WX
NPCT650CA0WX	NPCT650DA0WX	NPCT650HA0WX	NPCT650IA0WX
NPCT650LA0WX	NPCT650MA0WX	NPCT650NA0WX	NPCT650RA0WX
NPCT650SA0WX	NPCT650TA0WX	NPCT650UA0WX	NPCT650VA0WX
NPCT650JA0WX	NPCT652AA0WX	NPCT652BA0WX	NPCT652CA0WX
NPCT652DA0WX	NPCT652HA0WX	NPCT652IA0WX	NPCT652LA0WX
NPCT652MA0WX	NPCT652NA0WX	NPCT652RA0WX	NPCT652SA0WX
NPCT652TA0WX	NPCT652UA0WX	NPCT652VA0WX	NPCT652JA0WX
NPCT650AA0YX	NPCT650BA0YX	NPCT650CA0YX	NPCT650DA0YX
NPCT650HA0YX	NPCT650IA0YX	NPCT650LA0YX	NPCT650MA0YX
NPCT650NA0YX	NPCT650RA0YX	NPCT650SA0YX	NPCT650TA0YX
NPCT650UA0YX	NPCT650VA0YX	NPCT650JA0YX	NPCT652AA0YX
NPCT652BA0YX	NPCT652CA0YX	NPCT652DA0YX	NPCT652HA0YX
NPCT652IA0YX	NPCT652LA0YX	NPCT652MA0YX	NPCT652NA0YX
NPCT652RA0YX	NPCT652SA0YX	NPCT652TA0YX	NPCT652UA0YX
NPCT652VA0YX	NPCT652JA0YX		

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit sont principalement ceux décrits par le profil de protection [BSI-CC-PP-0030-2008-MA-01] :

- l'exécution des instructions TPM et l'implémentation de la machine d'état TPM ;
- l'authentification de l'entité propriétaire ;
- la gestion des registres de configuration (PCR[1]) ;
- la génération, l'exportation et l'importation de fichiers chiffrés (BLOB[2]) contenant des données du type : clés, valeurs de registres de configuration, etc. ;
- la configuration de sécurité ;
- la gestion de délégation et la gestion de la localité ;
- l'accès aux fonctions cryptographiques (RSA, AES, SHA1, HMAC, MGF1) ;
- le stockage de la paire de clés EK[3] ;
- la génération de clés et le stockage des clés (SRK[4], User Keys) ;
- la génération de nombres aléatoires ;
- la gestion des compteurs (*tick counters*, *monotonic counter*) ;
- la séquence de démarrage et l'auto-test ;
- la protection physique par un bouclier actif (*active shield*) ;
- la mise à jour du logiciel embarqué sur le produit.

1.2.4. Architecture

L'architecture matérielle du composant « TPM 1.2, Hardware version FB5C85D, Firmware version 5.81.0.0 » est illustrée par la figure 1.

Le composant est constitué des modules suivants :

- une unité centrale ;

[1] *Platform Configuration Register.*
[2] *Binary Large Object.*
[3] *Endorsement Key.*
[4] *Storage Root Key.*

- des unités d'interfaces LPC[1], SPI[2], I2C[3], GPIO[4] ;
- un générateur de nombres aléatoires ;
- des modules d'accélération cryptographique pour le support des calculs RSA, AES, SHA-1 ;
- des blocs mémoires de type ROM (44 Koctets), RAM (32 Koctets) et OTP[5] (128 octets) ;
- un bloc *Timers ;*
- un ensemble de détecteurs de sécurité (*glitch*, tension, etc.).

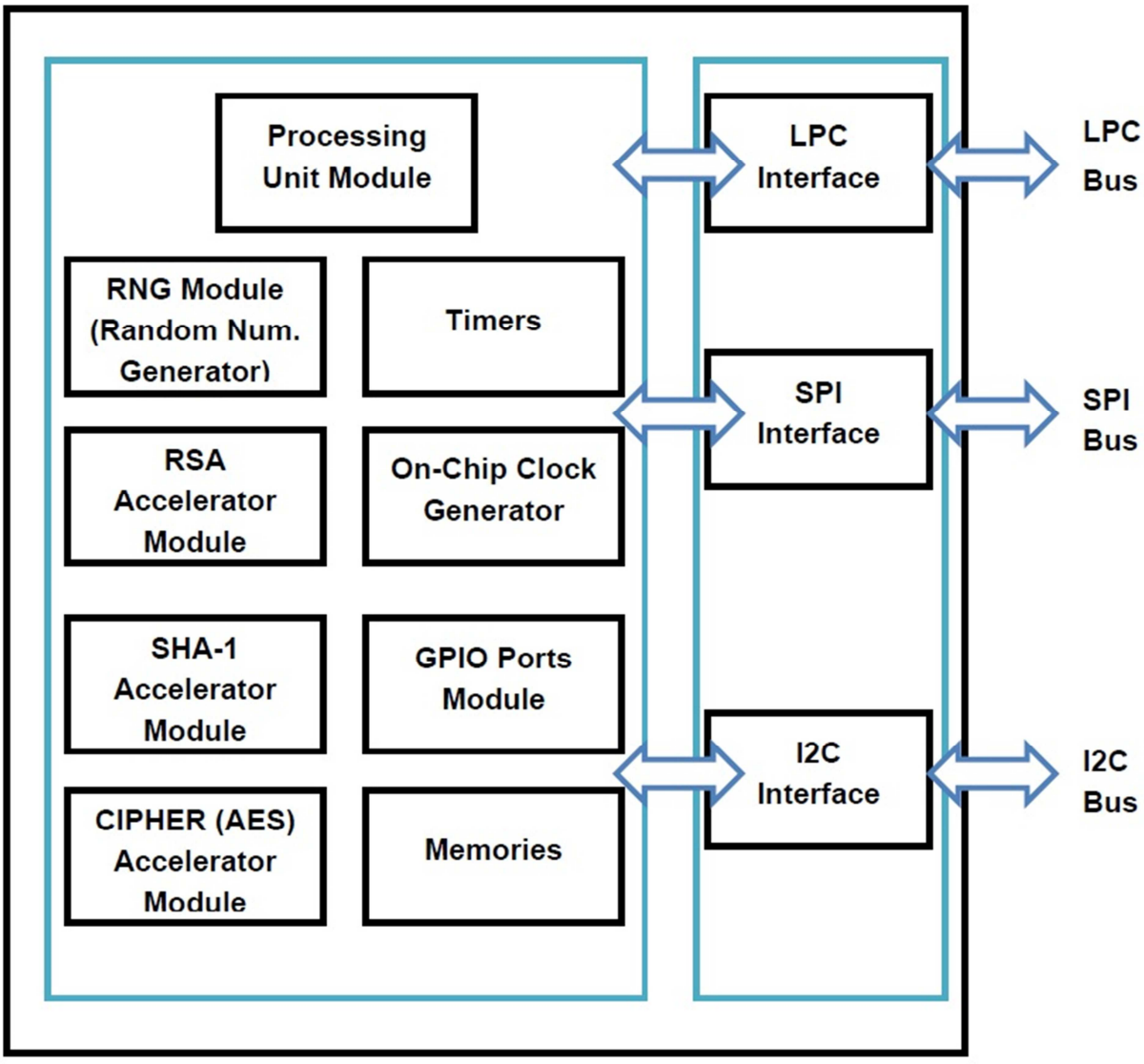

Figure 1. Architecture

[1] *Low Pin Count.*
[2] *SerialPeripheral Interface.*
[3] *Inter Integrated Circuit.*
[4] *General Purpose Input Output.*
[5] *One-Time Programmable.*

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]).

Le produit a été développé et fabriqué sur les sites suivants :

Nuvoton Technology Israel
Design Center Hasadnaot 8,
Hertzelia, Israel

Nuvoton Technology Israel
Design Center2 Ataa'sia 8, Ramat Gavriel,
Migdal Haemek, Israël

Trusted Labs
5 rue du Bailliage,
78000 Versailles, France

TOPPAN Photomasks France
Mask Fab, 224 Bld JF Kennedy,
91105 Corbeil-Essonnes Cedex, France

TOPPAN Photomasks Germany
Mask Fab Germany
Rähnitzer Allee 9,
01109 Dresden, Germany

TSL Wafer Fab
Ramat Gavriel Industrial
Area, MigdalHaemek, Israël

ASE Group Chung-Li
Assembly plants, 550, Chung-Hwa Road,
Section 1, Chung-Li, 320,
Taiwan, République de Chine

AMKOR Technology Philippines, Inc.
Assembly plants,. (ATP) - P1, KM 22 East
Service Road, Special Economic Zone,
Cupang, Muntinlupa City, 1702, Philippines

AMKOR Technology Philippines, Inc.
Assembly plants, (ATP) - P3/P4, 119 North
Science Avenue, Special Economic
Processing Zone, Laguna Technopark,
Binan Laguna, 4024, Philippines

NTC Wafer test and final test plant No. 4,
Creation Rd. III, Hsinchu Science Park,
Taiwan, République de Chine

1.2.6. Configuration évaluée

Le certificat porte sur le composant programmé avec l'application TPM, tel que présenté plus haut au paragraphe « Architecture » et configuré conformément au guide de personnalisation (cf. [GUIDES]). Le composant a été testé en mode opérationnel qui est le mode dans lequel il est livré à l'utilisateur, conformément au profil de protection [BSI-CC-PP-0030-2008-MA-01].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [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 composants pour cartes à puce et produits assimilés, 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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 avril 2015, 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 vulnérabilités de conception et de construction pour le niveau AVA_VAN.4 visé.

2.4. Analyse du générateur d'aléas

Pour le niveau AVA_VAN.4 visé, l'évaluation n'a pas mis en évidence de vulnérabilités exploitables du générateur d'aléas.

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 « TPM 1.2, Hardware version FB5C85D, Firmware version 5.81.0.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 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].

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'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 :

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 signataires[2], des certificats Critères Communs.
Pour les évaluations enregistrées avant septembre 2014, 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, Singapour, la Suède et la Turquie.

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**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**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**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	2	**2**	**2**	Sufficiency of security measures
	ALC_FLR								**1**	Basic Flaw Remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**4**	Moderate vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target TPM 1.2, version 0.65, 22 April 2015, Nuvoton Technology. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite 1.1, version 1.2, April 2015, Nuvoton Technology.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report TPM1.2bis project, reference TPM1.2bis_ETR_v1.2, version 1.2, 24 April 2015, Serma Technologies.
[CONF]	Liste de configuration du produit : - ALC_Doc_Report, version 1.0, Nuvoton Technology ; - ArsufIC_ALC_CMS.1, version 1.04, Nuvoton Technology.
[GUIDES]	Guide d'installation du produit : - NPCT6xx TPM Initialization and Configuration Application Note, June 2014, Nuvoton Technology. Guides d'administration du produit : - NPCT62x LPC/SPI/I2C Trusted Platform Module (TPM) datasheet, version 0.88, April 2014, Nuvoton Technology ; - NPCT62x/NPCT65x TPM1.2 with LPC, SPI and I2C Interfaces programmer's Guide, version 1.0, January 2014, Nuvoton Technology. Guide d'utilisation du produit : - ARSUF (NPCT6xynA0 TPM 1.2) Operational Guidance Document, version 1.0, 3rd July 2014, Nuvoton Technology.
[BSI-CC-PP-0030-2008-MA-01]	Protection Profile - PC Client Specific Trusted Platform Module, TPM Family 1.2, version v1.2. 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 6 octobre 2011 sous la référence BSI-CC-PP-0030-2008-MA-01.

Annexe 3. Références liées à la certification

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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir http://www.ssi.gouv.fr.

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