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-2018/61

NPCT7xx TPM2.0 rev1.38
Hardware version LAG019
Firmware version 7.2.1.0

Paris, le 18 janvier 2019

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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@ssi.gouv.fr

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

Référence du rapport de certification

ANSSI-CC-2018/61

Nom du produit

NPCT7xx TPM2.0 rev1.38

Référence/version du produit

Hardware LAG019
Firmware 7.2.1.0

Conformité à un profil de protection

PC Client Specific Trusted Platform Module, Family 2.0, Level 0, Revision 1.38, version 1.1.

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

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 Safety & Security

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

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

SOG-IS

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. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 7
1.2.4. Identification du produit 8
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 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. Reconnaissance européenne (SOG-IS) 12
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 14

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 15

1. Le produit

1.1. Présentation du produit

Le produit évalué est « NPCT7xx TPM2.0 rev1.38, Hardware version LAG019, Firmware version 7.2.1.0 » 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 TPM 2.0 (*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 [PP-TM].

1.2.2. Services de sécurité

Les services de sécurité fournis par le produit sont ceux décrits dans la cible de sécurité [ST], à savoir :

- l'accès aux fonctions cryptographiques (RSA, AES, ECC, 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

L'architecture matérielle du composant « NPCT7xx TPM2.0 rev1.38, Hardware version LAG019, Firmware version 7.2.1.0 » est illustrée par la figure 1.

Le composant est constitué principalement :

- d'une unité centrale ;
- des unités d'interfaces GPIO[1], SPI[2], I2C[3] ;
- d'un générateur de nombres aléatoires ;
- des modules d'accélération cryptographique pour le support des calculs RSA/ECC, AES, SHA-1/SHA-256 ;
- des blocs mémoires de type ROM, RAM, Flash ;
- d'un bloc *Timers.*

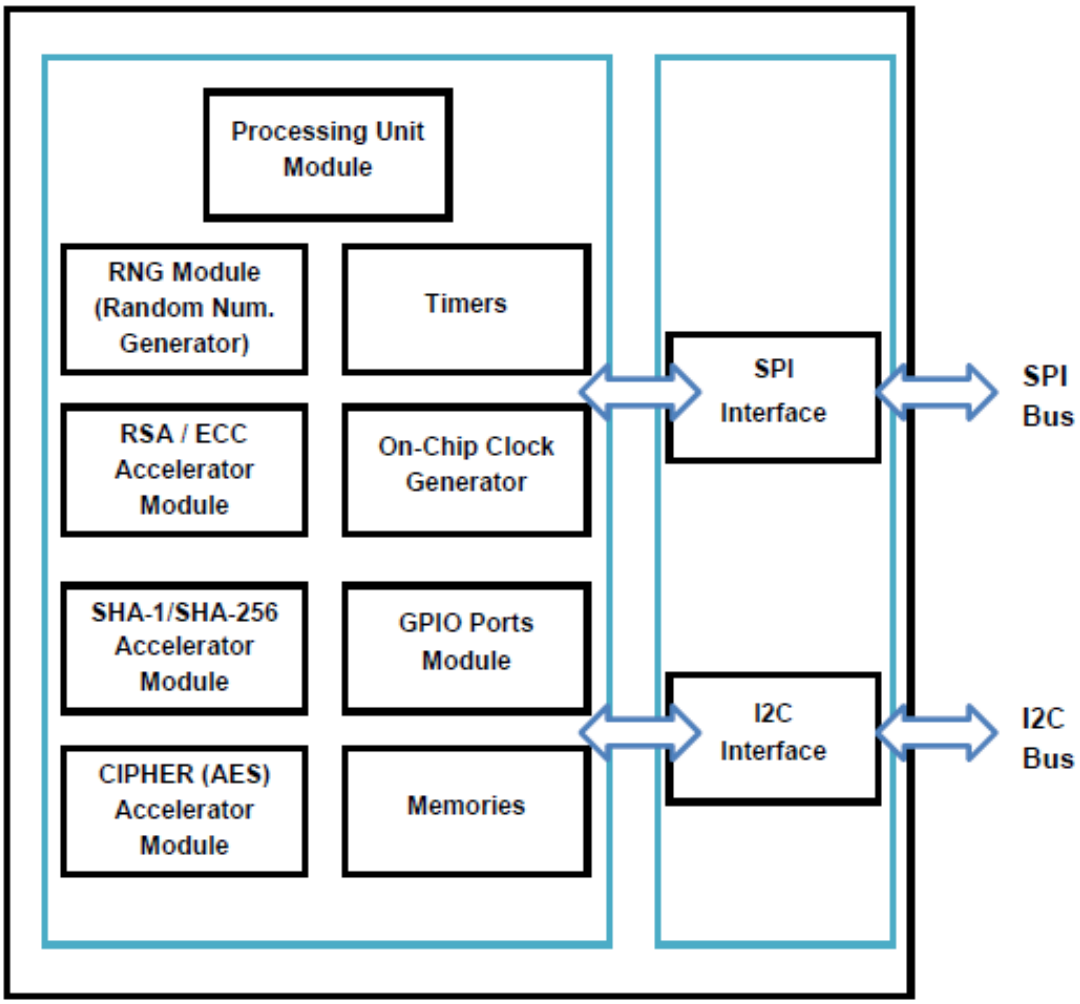

Figure 1. Architecture

[1] *General Purpose Input Output.*
[2] *SerialPeripheral Interface.*
[3] *Inter Integrated Circuit.*

1.2.4. 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 :

- la version matérielle « LAG019 » est identifiée par les registres (voir [ST] §1.1) :
  - VID = 0x1050 ;
  - DID = 0x00FC ;
  - RID = 0x01.
- La version matérielle est également inscrite sur le composant : NPCT7xx (voir [GUIDES]) ;
- la version logicielle est obtenue à l'aide de la commande « TPM2_GetCapability » qui retourne les données identifiant la version *firmware* 7.2.1.0 (voir [ST] §1.1). La version logicielle est associée aux données suivantes :
  - *firmware* v2.1.0.36 ;
  - *cryptolib* v2.0.18 ;
  - *booter* v2.0.7 ;
  - *bootloader* v2.0.0.21.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]), qui est conforme au profil de protection [PP-TPM] :

- phase 1 : développement du TMP (spécification du circuit intégré, du logiciel dédié et du *firmware*) ;
- phase 2 : fabrication et livraison du TPM ;
- phase 3 : intégration de la plateforme ;
- phase 4 : utilisation opérationnelle.

Les phases 1 et 2 sont couvertes par les classes d'assurances ALC, tandis que les phases 3 et 4 sont couvertes par les guides [GUIDES].
Aux phases 3 et 4, la fonctionnalité de mise à jour du *firmware* sur le terrain est disponible. Elle nécessite une autorisation du *firmware* ainsi qu'une vérification de l'intégrité et l'authentification des données de mise à jour authentiques fournies par *NUVOTON TECHNOLOGY ISRAEL LTD.*

Le produit a été développé, fabriqué et expédié sur les sites décrit par la figure 2.

L'évaluation couvre la configuration finale du produit, i.e. celle obtenue en phase 4.

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 and 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 du produit

1.2.6. Configuration évaluée

Le certificat porte sur le composant programmé avec l'application TPM 2.0, tel que présenté 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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 11 décembre 2018, 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 TPM2.0 rev1.38, Hardware version LAG019, Firmware version 7.2.1.0 » 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'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour certains équipements matériels avec boîtiers sécurisés, 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 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] 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**	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 : - NPCT7xx TPM2.0 Security Target, référence NPCT7xx_TPM2.0_rev1.38_Nuvoton_ST_Internal_v1.0.3, reference 1.0.3, 4/09/2018. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - NPCT7xx TPM2.0 rev 1.38 Security, référence NPCT7xx_TPM2.0_rev1.38_Nuvoton_ST_External_v1.0.3, version 1.0.3, 4/09/2018.
[RTE]	Rapport technique d'évaluation : Evaluation Technical Report – NPCT7_2 project, référence, NPCT7_2_ETR_v1.2, version 1.2, 11/12/2018.
[CONF]	Liste de configuration du produit : - CM scope, NPCT7xx_TPM2.0_rev1.38_IC_ALC_CMS.1, version 1.0.2, 30/08/2018 ; - NPCT7xx_TPM2.0_Doc_Report, version 2.2, 4/09/2018 reports ; - NPCT7xx_Issues_DB_Snapshot, version 1.0, 30/10/2017.
[GUIDES]	- NPCT75xxAB TPM2.0 Guidance Document, Common Criteria AGD Component, version 1.1, 2/09/2018 ; - NPCT75x Trusted Platform Module Family 2.0 – Datasheet, référence NPCT75x_DS_Rev1.5, version 1.5, 04/2018 ; - NPCT75x- User Product Information, référence NPCT75x_Errata_Rev2.1, version 2.1, 2/09/2018 ; - NPCT75x TPM2.0 Programmer's Guide, référence NPCT75x_TPM2 0_ProgGuide_Rev.1.1, version 1.1, 17/05/2018.
[PP-TPM]	Protection Profile - PC Client Specific Trusted Platform Module, TPM Library specification Family 2.0, Level 0, Revision 1.38, version 1.1. *Certifié par l'ANSSI le 10 août 2018 sous la référence ANSSI-CC-PP-2018/03.*

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 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.
[CC]	Common Criteria for Information Technology Security Evaluation : - 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]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir 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.