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-2016/78

ST33TPHF2ESPI mode TPM 2.0
TPM Firmware version 73.00

Paris, le 13 décembre 2016

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

Guillaume POUPARD
[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 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

Référence du rapport de certification

ANSSI-CC-2016/78

Nom du produit

ST33TPHF2ESPI mode TPM 2.0

Référence/version du produit

Hardware ST33HTPH révision A/C (Externe/Interne), TPM Firmware 73.00

Conformité à un profil de protection

[PP-TPM]
PC Client Specific Trusted Platform Module (Family 2.0, Level 0, Revision 1.16)

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté
ALC_FLR.1, AVA_VAN.4

Développeur

STMicroelectronics
Green Square Building B, Lambroekstraat, 5, B-1831 Diegem, Belgique

Commanditaire

STMicroelectronics
Green Square Building B, Lambroekstraat,5, B-1831 Diegem, Belgique

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI 1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 « ST33TPHF2ESPI mode TPM 2.0, hardware ST33HTPH révision A en externe et C en interne, TPM[1] *firmware* version 73.00[2] » développé par la société *STMICROELECTRONICS.*

Ce produit est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs, etc.) conformément aux spécifications fonctionnelles TPM[3] 2.0.

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 principalement ceux décrits dans le profil de protection [PP-TPM] :

- l'exécution des instructions TPM et l'implémentation de la machine d'état TPM ;
- le contrôle de l'intégrité d'objets protégés importés dans le TPM ;
- la protection de la confidentialité d'objets (BLOB[4]) protégés exportés depuis le TPM ;
- la protection physique des objets protégés résidant dans le TPM ;
- l'authentification de l'entité propriétaire ;
- la gestion des registres de configuration (PCR[5]) ;
- la gestion de délégation et la gestion de la localité ;
- le stockage de la paire de clés EK[6] ;
- la génération de clés et le stockage des clés (SRK[7], *User Keys, PSS*[8]) ;
- l'accès à des services cryptographiques dont les primitives sont supportées par la nouvelle librairie NesLib 5.1.0 et par les modules cryptographiques matériels : AES 128 mode CTR et CFB, signature chiffrement PKCS, MGF et dérivation de clé ;
- la génération de nombres aléatoires ;
- la signature RSA et ECC ;
- la destruction des valeurs de clés générées ;

[1] *Trusted Platform Module.*
[2] 49.00 en hexadecimal.
[3] *Trusted Platform Module.*
[4] *Binary Large Object.*
[5] *Platform Configuration register.*
[6] *Endorsement Key.*
[7] *Storage Root Key.*
[8] *Platform Primary Seed.*

- la génération et la vérification des valeurs MAC (RSA, HMAC) et des HASH (SHA_1, SHA_256) ;
- la gestion des compteurs (*monotonic counter*) ;
- la séquence de démarrage et l'auto-test ;
- la mise à jour du logiciel embarqué sur le produit conformément à [NOTE6.2].

1.2.3. Architecture

L'architecture matérielle de la TOE est la suivante :

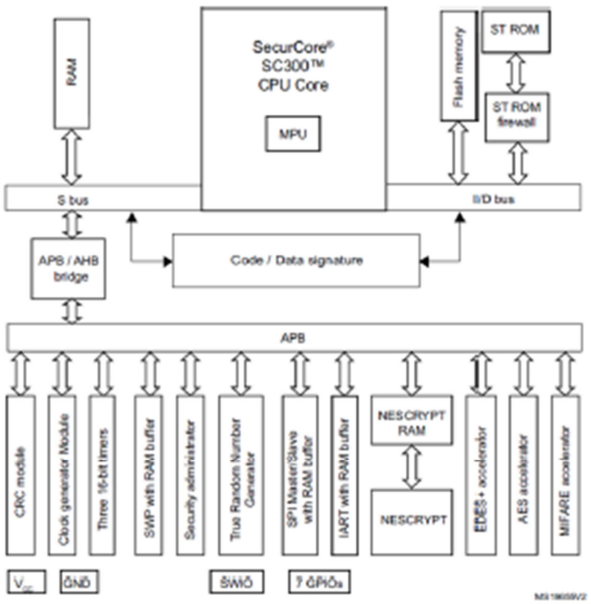

Figure 1 – Architecture *hardware*

Elle est composée :

- d'un processeur ARM® SecurCore® SC300™ 32-bit RISC core basé sur un CORTEX™ M3 core ;
- de mémoires : FLASH, ROM et RAM ;
- de modules fonctionnels : compteurs, bloc de gestion d'interface série SPI[1] ;
- de modules de sécurité : unité de protection des mémoires (MPU[2]), générateur de nombres aléatoires (TRNG), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, unité de protection physique par un bouclier actif (*active shield*) et détection de fautes ;
- de coprocesseurs :
  - EDES pour le support des algorithmes DES ;
  - AES pour le support des algorithmes AES ;
  - NESCRYPT muni d'une RAM dédiée pour le support des algorithmes cryptographiques à clé publique,
- d'une mémoire non volatile (ROM) protégée par un *firewall* qui contient :
  - un programme d'autotest dédié à la validation de la TOE en production (OST v2.2) ;

[1] *Serial Peripherical Interface*
[2] *Memory Protection Unit*

- un jeu de tests dédié au démarrage du composant (*boot sequence*) et à la gestion des services en mémoire FLASH.

L'architecture *firmware* est la suivante :

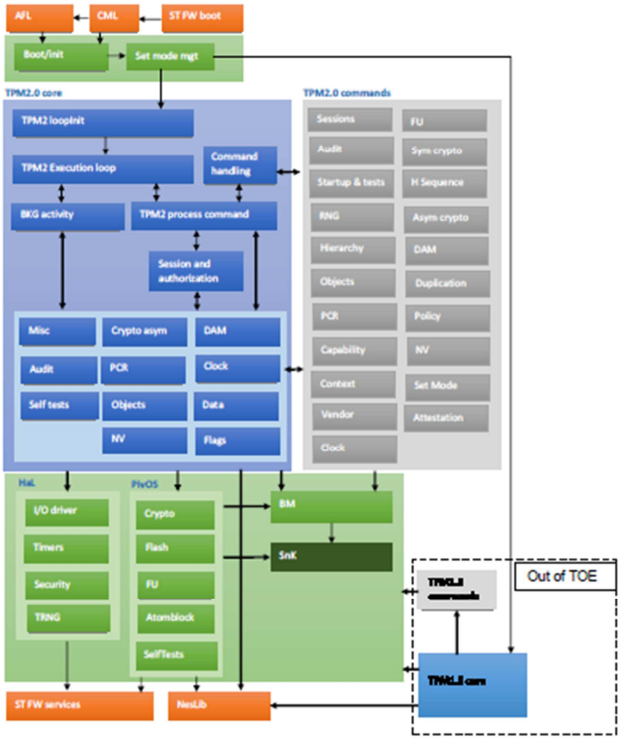

Figure 2 – Architecture *firmware*

La TOE *firmware* « F2E » est divisée en plusieurs modules :

- le PivOS qui est module supportant un ensemble de services de bas niveau ;
- la *Hardware Abstraction Layer (*HaL) qui est un ensemble de services fourni par la plate-forme *hardware* ;
- le *Block Manager* (BM) qui est un module supportant les services « tampon » pour le stockage des données ;
- le *Secure nano kernel* (Snk) supportant les services de bas niveaux pour les nano cellules de cryptographie symétrique et pour les transactions atomiques ;
- le TPM 2.0 *core* ;
- le TPM 2.0 *commands* ;
- la librairie cryptographique NesLib version 5.1.0.

Note : le firmware intègre également les modules TPM1.2 *commands* et TPM1.2 *core* qui sont hors périmètre de la TOE pour pouvoir revendiquer la conformité au profil de protection « « PC Client Specific Trusted Platform Module, family 2.0, level 0, révision 1.16, version1.0 ».

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 (voir [ST] et [GUIDES]) :

- La dénomination commerciale du composant ST33TPHF2ESPI pour cette version de *firmware* est, soit « P68HAAF1 **»** (produit en mode TPM 2.0 par défaut) ou « P68HAAF0 » (produit en mode TPM 1.2 par défaut configuré en mode TPM 2.0) ;

- informations inscrites sur la surface du composant :
  - *maskset reference* : **K8K0** ;
  - *OST[1] revision (autotest ROM code) : OST 2.2 (***YQBF***) ;*
- contenu de « TMP_CAP_VENDOR_PROPERTY » obtenu à partir de la commande « TMP_GetCapability » :
  - *hardware Chameleon code :* **41 46 31 00 (AF1 pour TPM 2.0)** ou **41 46 30 00 (AF0 pour TPM 1.2)** ;
  - *digest factory* (32 bytes) : 30 A2 14 ED F6 3A 25 DB 9A 9B BC AC F1 45 DC E4 A2 7A DF EA 64 CA 79 1A 11 57 B6 F1 A8 A4 3D 50 ;
  - *digest current* (32 bytes) : 30 A2 14 ED F6 3A 25 DB 9A 9B BC AC F1 45 DC E4 A2 7A DF EA 64 CA 79 1A 11 57 B6 F1 A8 A4 3D 50 ;
- contenu de « TMP_CAP_TPM_PROPERTIES» obtenu à partir de la commande « TMP_GetCapability » :
  - *TMP firmware version :* 01 49 00 00 ;
  - *internal firmware version :* 44 A0 0F 17.

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 est fabriqué sur les sites suivants :

STMICROELECTRONICS Smartcard IC division 190, avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	***STMICROELECTRONICS*** 18 Ang Mo Kio Industrial park 2, 569505 Singapour
STMICROELECTRONICS 10, rue de Jouanet ePark 35700 Rennes France	***STMICROELECTRONICS*** Green Square Lambroekstraat 5, Building B, 3rd floor, 1831 Diegem/Machelen Belgique
STMICROELECTRONICS 850, rue Jean Monnet 38926 Crolles France	***STMICROELECTRONICS*** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour

[1] *Operating System for Test.*

1.2.6. Configuration évaluée

Le certificat porte sur le composant « ST33TPHF2ESPI mode TPM 2.0, hardware ST33HTPH révision A en externe et C en interne, *firmware* version 73.00 », tel que présenté précédemment aux paragraphes 1.2.2, 1.2.3 et 1.2.4 et configuré conformément aux guides [GUIDES].

Le marquage externe « P68HAAF1 » mentionné sur le boîtier du composant indique que le TPM2.0 est activé par défaut en sortie d'usine. L'utilisateur peut néanmoins commuter ce produit en TMP1.2 (hors périmètre de certification) à l'aide de la commande *SetMode* (voir GUIDES]) sans que le code c*hameleon* ne soit modifié pour autant. Pour pouvoir vérifier la configuration du mode supporté par le TPM, il est alors nécessaire de s'assurer qu'une commande TPM 1.2 définie dans la librairie TPM 1.2 telle que TPM_Startup, s'exécute effectivement ou qu'une commande définie dans la librairie TPM 2.0 telle que TPM2_Startup, ne s'exécute plus correctement. Le processus inverse s'applique également lorsque le composant est commuté de TPM 1.2 en TPM 2.0.

Concernant la librairie Neslib 5.1, seules les fonctions utilisées pour les besoins de l'application TPM, ont été évaluées.

Le composant ST33TPHF2ESPI a été testé en mode opérationnel à l'identique de ceux livrés aux clients finaux.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM] et à la note [NOTE6.2].

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

L'évaluation s'appuie :

- pour le *hardware*, sur les résultats d'évaluation du produit certifié par l'ANSSI sous la référence [CER-2015/36] ;
- pour le *software* embarqué, sur certains résultats d'évaluations des produits certifiés par l'ANSSI sous les références [CER-2015/80], [CER-2016/43] et [CER-2016/44].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 novembre 2016, 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

Le générateur de nombres aléatoires n'a pas fait l'objet d'une nouvelle évaluation selon la méthodologie [AIS 31] dans la mesure où ce même générateur avait été déjà évalué lors de la certification des produits [CER-2016/43] et [CER-2016/44]. Pour mémoire, ce générateur répond aux exigences de la classe DRG3.

Les résultats précédents 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 « ST33TPHF2ESPI mode TPM 2.0, Hardware ST33HTPH révision A (externe) et C (interne), TPM Firmware version 73.00 » soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_FLR.1, 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 par 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 les cartes à puces 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 :

[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.

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[1], 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] 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, le Qatar, 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	**1**	Sufficiency of security measures
	ALC_FLR				**1**				**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 : - ST33TPHF2ESPI_M20_FW4900_ST, référence SSS_ST33TPHF2ESPI_M20_ST_16_002, version 01-01 du 10 novembre 2016, STMicroelectronics. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33TPHF2ESPI_M20_FW4900_ST, référence SSS_ST33TPHF2ESPI_M20_STP_16_002, version 01-01p du 10 novembre 2016, STMicroelectronics.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – Grenache 2.0 V2, référence GRE20_ETR, version 2.0 du 28 novembre 2016, Thales.
[CONF]	Liste de configuration du produit : - TPM firmware F2E 0x49 0x00 for chip "AF0 & AF1" configuration list, référence SSS_TPMF2E_4900_AF01_CFGL_16_001, version 01-00 du 7 novembre 2016, *STMICROELECTRONICS.* - ST33HTPH rev C & ST_Firmware rev1(ext) rev1(int) configuration list, référence SMD_33HTPM_HTPH_CFGL_16_001, version 01.01, *STMICROELECTRONICS*.
[GUIDES]	- Datasheet - Flash based device combining TPM 1.2 and TPM 2.0 with and SPI interface, référence DS_ST33TPHF2ESPI, version 8 d'août 2016, *STMICROELECTRONICS*. - ST33TPMF2E – Security Guidelines for TPM Configuration, référence SSS_ST33TPMF2E_AN_15_005, version 01-03 du 18 décembre 2015, *STMICROELECTRONICS*. - ST33TPHF2ESPI – FW 49.00, AGD deliveries, référence SSS_ST33TPHF2ESPI_4900_AGD_16_001, version 01-00 du 28 octobre 2016, *STMICROELECTRONICS*. - STSW-TPMCERT1 – ST Trusted Platform Module Endorsement Key certificates, référence DocID028078, version 3 de septembre 2016, *STMICROELECTRONICS*. - ST33TPHF20SPI Security recommendations, référence SSS_TPHF20_AN_16_001, version 01-02 du 27 octobre 2016, *STMICROELECTRONICS*.
[PP-TPM]	Profil de protection – PC Client Specific Trust Platform Module, family 2.0, level 0, revision 1.16, version 1.0, 6 mai 2015. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2015/07.*
[CER-2016/44]	Rapport de certification ANSSI-CC-2016/44 « ST33TPHF2ESPI mode TPM 1.2, TPM Firmware versions 47.00 et 47.04 », émis le 4 juillet 2016, ANSSI.
[CER-2016/43]	Rapport de certification ANSSI-CC-2016/43 « ST33TPHF2ESPI mode TPM 2.0 TPM Firmware versions 47.00 et 47.04», émis le 4 juillet 2016, ANSSI.

[CER-2015/36]	Rapport de certification ANSSI-CC-2015/36 « Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1 », émis le 15 septembre 2015, ANSSI.
[CER-2015/80]	Rapport de certification ANSSI-CC-2015/80 du TPM « ST33TPMF2ESPI », émis le 29 janvier 2016, ANSSI.

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.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[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.
[NOTE6.2]	Note d'application n°6 « Exigences de sécurité pour un chargement de code en phase d'utilisation », version 2.0, 23 janvier 2015, ANSSI.

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