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-2019/37

ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256
ST33GTMPA with TPM Firmware 3.256 & 6.256

Paris, le 18 octobre 2019

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2019/37

Nom du produit

ST33TPHF2X & ST33GTPMA

Référence/version du produit

ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTMPA with TPM Firmware 3.256 & 6.256

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_FLR.1, AVA_VAN.5

Développeur

STMicroelectronics

10 rue de Jouanet, 35700 Rennes, France

Commanditaire

ProtonWorld Intl, filiale de STMicroelectronics NV

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

Centre d'évaluation

THALES / CNES

290 allée du Lac, 31670 Labège, France

Accords de reconnaissance applicables

CCRA

SOG-IS

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

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

Les produits évalués sont « ST33TPHF2X & ST33GTPMA, ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTMPA with TPM Firmware 3.256 & 6.256 » développés par STMicroelectronics.

Le ST33TPHF2X correspond à une gamme de *Trusted Platform Modules* (TPM). Cette gamme de produits est destinée à apporter des services de sécurité (démarrage sécurisé, génération et stockage de clés cryptographiques, génération de signature et certificats, calcul de haché et génération de nombre aléatoire) aux ordinateurs personnels, serveurs et imprimantes. Ces TPM se déclinent sur une plateforme matérielle ST33HTPH en version A.C, avec une interface SPI (*firmwares* versions 1.256 et 1.257) et I²C (*firmware* 2.256).

Le ST33GTPMA correspond également à une gamme de *Trusted Platform Modules*. Cette gamme est quant à elle destinée au marché de l'automobile et apportent des services similaires. Ces TPM se déclinent sur une plateforme matérielle ST33G1M2A0 en version F.G, également avec une interface SPI (*firmware* version 3.256) et I²C (*firmware* 6.256).

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] et sont listés dans la cible de sécurité [ST] :

- 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 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 ;
- la gestion de délégation et la gestion de la localité ;
- le stockage de la paire de clés EK (*Endorsment Key)* ;
- la génération et le stockage des clés *Storage Root Key*, *user keys* et *Platform Primary Seed* ;
- différents services cryptographiques dont les primitives sont supportées par la bibliothèque NesLib 6.3.3 :
    - le hachage avec les algorithmes SHA-256, SHA-384, SHA-1, SHA-3-256 et SHA-3-384 ;
    - le chiffrement asymétrique, la signature et le partage de secret avec RSA 2048 ;

- la signature asymétrique ECDSA et le partage de secret ECDH sur les courbes elliptiques P-256, P-384, et BN-256 ;
- le chiffrement symétrique AES avec des clés de 128, 192 et 256 bits, en modes ECB, CBC, CTR, CFB et OFB ;
- la génération et vérification de signature symétrique par HMAC.

1.2.3. Architecture

L'architecture matérielle de la TOE est la suivante :

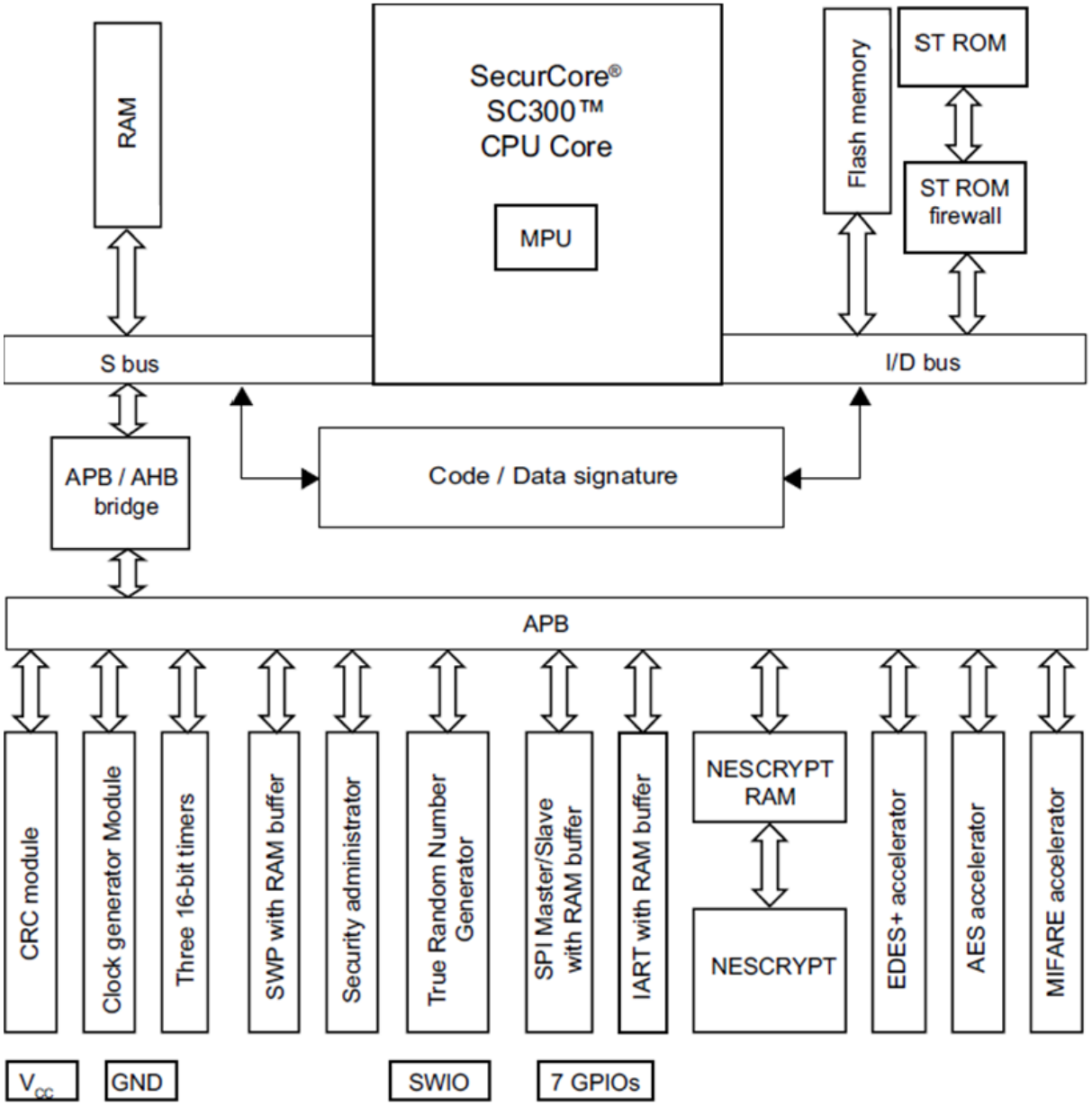


Figure 1 – Architecture matérielle

Elle est composée :

- d'un processeur ARM® SecurCore® SC300™ 32-bit RISC core basé sur un Cortex™ M3 core ;
- de mémoires : RAM, FLASH et ROM ;
- de modules fonctionnels : compteurs, bloc de gestion d'interface série I²C et SPI ;

- de modules de sécurité : unité de protection des mémoires (MPU), 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 pare-feu qui contient :
  - un programme d'autotest dédié à la validation de la TOE en production (OST version 2.2) ;
  - 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 :

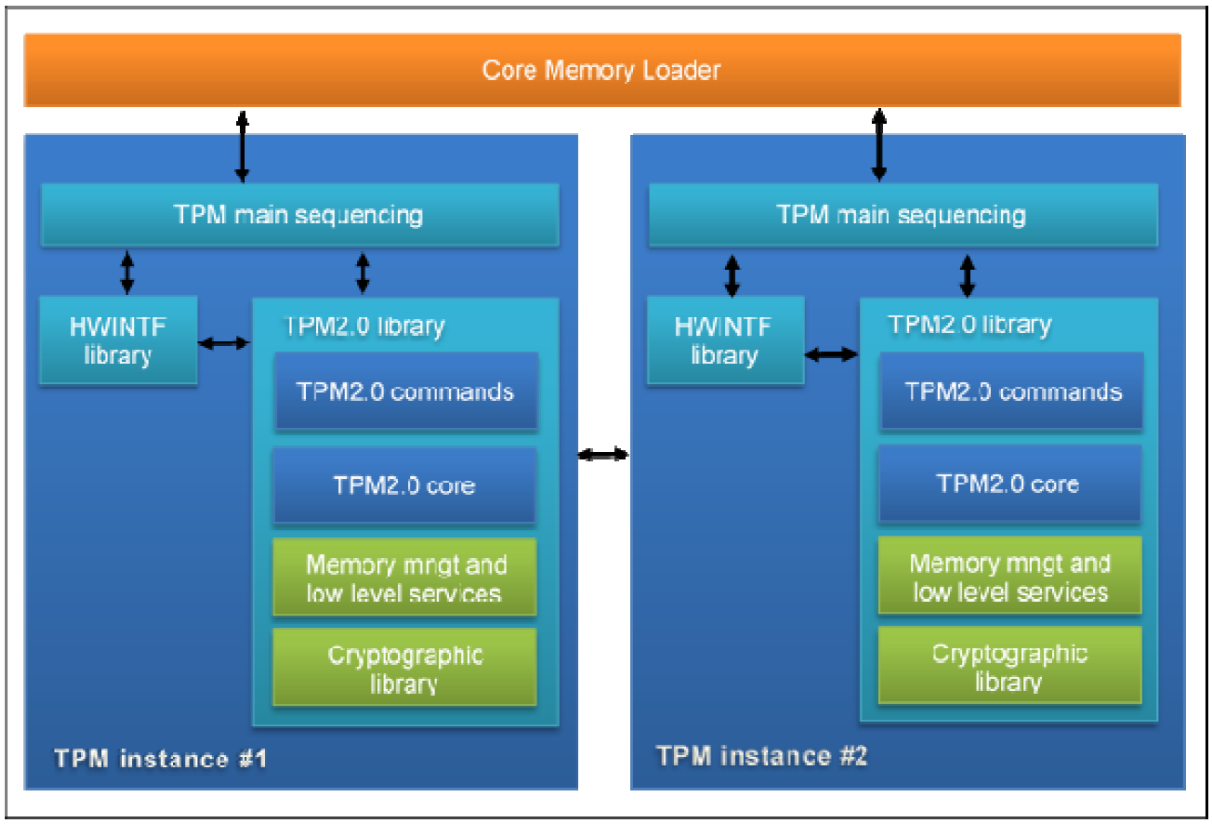


Figure 2 – Architecture logicielle

Elle est composée :

- d'un bloc de code non modifiable situé en ROM et en FLASH, contenant le *core memory loader*, chargé de vérifier l'intégrité de l'instance TPM à exécuter ;
- de deux blocs de code modifiable, dont seulement l'une des deux instances TPM implémentées par ces blocs s'exécute. Cette double instanciation du TPM permet une mise à jour sécurisée.

1.2.4. Identification du produit

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

Les versions certifiées des produits sont identifiables en utilisant la commande « TPM2_GetCapability » afin d'obtenir les valeurs de « TPM_CAP_VENDOR_PROPERTY » :

- pour ST33TPHF2X :
  - avec interface SPI :
    - *firmware* 1.256, voir *Appendix* A de [DS_1.256] ;
    - *firmware* 1.257, voir *Appendix* A de [DS_1.257] ;
  - avec interface I²C et *firmware* 2.256, voir *Appendix* A de [DS_2.256] ;
- pour ST33GTPMA :
  - avec interface SPI et *firmware* 3.256, voir *Appendix* A de [DS_3.256] ;
  - avec interface I²C et *firmware* 6.256, voir *Appendix* A de [DS_6.256] ;

Pour connaître les versions des produits, l'utilisateur peut également se référer au marquage inscrit sur le boitier (voir les guides correspondants, au paragraphe 15, pour les références).

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant correspond aux phases 1 et 2 du [PP-TPM], comme décrit dans la cible de sécurité ([ST]).

Le produit a été développé sur les sites suivant (voir [SITES]) :

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 Singapour
STMicroelectronics 10, rue de Jouanet ePark 35700 Rennes France	**STMicroelectronics** Green Square Lambroekstraat 5, Building B, 3rd floor 1831 Diegem/Machelen France
STMicroelectronics 850, rue Jean Monnet 38926 Crolles France	**STMicroelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour

1.2.6. Configuration évaluée

Le certificat porte d'une part sur le composant « ST33TPHF2X » avec *hardware* ST33HTPH version A.C, *firmware* 1.256 et 1.257 (avec interface SPI) et 2.256 (avec interface I²C) et d'autre part sur le composant « ST33GTPMA » avec *hardware* ST33G1M2A0 version F.G, *firmware* 3.256 (avec interface SPI) et 6.256 (avec interface I²C), tels que présentés aux paragraphes 1.2.2, 1.2.3 et 1.2.4 et configuré conformément aux guides [GUIDES].

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 :

- pour le *hardware* :
  - ST33HTPH, les résultats du produit certifié par l'ANSSI sous la référence [CER-2015/36] ;
  - ST33G1M2A0, les résultats du produit certifié par l'ANSSI sous la référence [CER-2017/02] ;
- pour la bibliothèque cryptographique NesLib et pour les applications TPM, les résultats des anciennes versions certifiées par l'ANSSI sous la référence [CER-2018/41].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 septembre 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.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires a fait l'objet d'une analyse selon la méthodologie [AIS31] montrant qu'il répondait aux exigences de la classe DRG.3.

Par ailleurs, 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.5 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 « ST33TPHF2X & ST33GTPMA, ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTMPA with TPM Firmware 3.256 & 6.256» 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_FLR.1 et AVA_VAN.5.

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].

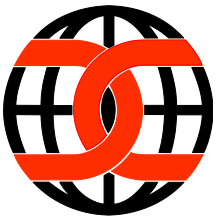
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

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

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] 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	**1**	Identification 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	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Trusted Platform modules ST33TPHF2X TPM FIRMWARE 1.256, 1.257 & 2.256 and ST33GTPMA TPM firmware 3.256 & 6.256 Security Target, référence SSS_ST33TPHF2X_GTPMA_ST_18_001, révision 01.01, daté du 26 juillet 2019, *STMICROELECTRONICS*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Trusted Platform modules ST33TPHF2X TPM FIRMWARE 1.256, 1.257 & 2.256 and ST33GTPMA TPM firmware 3.256 & 6.256 Security Target, référence SSS_ST33TPHF2X_GTPMA_ST_18_001 public, revision 01.01p, daté du 26 juillet 2019, *STMICROELECTRONICS*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – Project : AUXEY, référence AUX_ETR, version 1.3, daté du 5 septembre 2019, *THALES ;*
[CONF]	Liste de configuration du produit : - TPM FIRMWARE F2X 00.01.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HC4_CFGL_19_001, version 01-00, daté du 21 juin 2019, *STMICROELECTRONICS* ; - TPM FIRMWARE F2X HC5 00.02.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HC5_CFGL_19_001, version 01-00, daté du 5 juillet 2019, *STMICROELECTRONICS* ; - TPM FIRMWARE F2X HD4 0X00.01.01.01 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HD4_CFGL_19_001, version 01-00, daté du 27 juin 2019, *STMICROELECTRONICS* ; - TPM FIRMWARE F2X AE5 00.03.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_AE5_CFGL_19_001, version 01-00, daté du 25 juin 2019, *STMICROELECTRONICS* ; - TPM FIRMWARE F2X AE6 00.06.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_AE6_CFGL_19_001, version 01-00, daté du 26 juin 2019, *STMICROELECTRONICS*.

[GUIDES]	- [DS_1.256] ST33TPHF2XSPI Datasheet – production data : Flash-memory-based TPM 2.0 device with an SPI interface and extended features, référence DS_ST33TPHF2XSPI Rev 1, version 2, daté du 17 avril 2019, *STMICROELECTRONICS* ; - [DS_1.257] ST33TPHF2XSPI Datasheet – production data : Flash-memory-based TPM 2.0 device with an SPI interface and extended features, référence DS_ST33TPHF2XSPI Rev 3, version 3, daté du 24 juillet 2019, *STMICROELECTRONICS* ; - [DS_2.256] ST33TPHF2XI2C Datasheet – production data : Long-term evolution TPM 2.0 device with an I²C interface, référence DS_ST33TPHF2XI2C Rev 1, version 1, daté du 5 juillet 2019, *STMICROELECTRONICS* ; - [DS_3.256] ST33GTPMASPI Datasheet – production data : Flash-memory-based TPM 2.0 device for automative applications with an SPI interface, référence DS_ ST33GTPMASPI Rev 3, version 3, daté du 25 juillet 2019, *STMICROELECTRONICS* ; - [DS_6.256] ST33GTPMAI2C Datasheet – production data : Flash-memory-based TPM 2.0 device for automative applications with an I²C interface, référence DS_ ST33GTPMAI2C Rev 3, version 3, daté du 26 juillet 2019, *STMICROELECTRONICS* ; - TPM EK Certificate – Chip and EK authenticity verification, référence SSS_TPMEK_UM_15_001, version 2, daté du 11 mars 2016, *STMICROELECTRONICS* ; - ST33TPHF20SPI – Security recommendations, référence SSS_TPHF20_AN_16_001, version 1.2, daté du 27 octobre 2016, *STMICROELECTRONICS*.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - ALC Class Evaluation Report – C15P0036 Project, référence C15P0036_ALC_GEN_V2.0, version 2.0, daté du 11 juillet 2018, *SERMA SAFETY & SECURITY* ; - ALC Class Evaluation Report – C15P0036 Project, référence C15P0036_ALC_GEN_V1.0, version 1.0, daté du 2 juin 2018, *SERMA SAFETY & SECURITY* ; - ALC Class Evaluation Report – STM Project, référence STM_GEN_v2.0, version 2.0, daté du 21 décembre 2018, *SERMA SAFETY & SECURITY* ; - Site Visit Lite Report – STM ROUSSET site audit, référence 17-0317_STM-Rousset_SVR-M_v1.1, version 1.1, daté du 20 juillet 2018, *SERMA SAFETY & SECURITY* ; - Sites Visit Report Lite – STM AMK1, Loyang & Calamba site audits, référence 17-0317-STM_SVR-M_v1.0, version 1.0, daté du 20 décembre 2017, *SERMA SAFETY & SECURITY* ; - Site Visit Lite Report – Toa Payoh site audit, référence 17-0317_TPY_SVR-M_v1.0, version 1.0, daté du 12 mars 2018, *SERMA SAFETY & SECURITY* ; - Site Visit Lite Report – STM CROLLES site audit, référence STM_Crolles_SVR-M_v1.0, version 1.0, daté du 18 juillet 2018, *SERMA SAFETY & SECURITY* ; - Site Audit Technical Report – STM Zaventem site audit, référence STM_Zaventem_STAR_v1.0, version 1.0, daté du 8 mars 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report – STM Rennes, référence STM_RNS_STAR_v1.0, version 1.0, daté du 22 mai 2019, *SERMA SAFETY & SECURITY*.
[PP-TPM]	Profil de protection – PC Client Specific Trust Platform Module, TPM Library family 2.0, level 0, revision 1.38, version 1.1, 10/8/2018. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2018/03.*
[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-2017/02]	Rapport de certification ANSSI-CC-2017/02 « Microcontrôleurs sécurisés ST33G1M2A et ST33G1M2M révision G, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 4.2.10 », émis le 16 février 2017, *ANSSI*.
[CER-2018/41]	Rapport de certification ANSSI-CC-2018/41 « ST33TPHF2E mode TPM 2.0, TPM Firmware versions 73.08 et 73.09 » émis le 24 septembre 2018, *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 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 3.0, avril 2019.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, mai 2018.
[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.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

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