



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-2019/46**

### **ST33TPHF20 TPM Firmware 0x4A.0x40 & 0x4A.0x41**

*Paris, le 7 novembre 2019*

*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 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](mailto:certification@ssi.gouv.fr)

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

Référence du rapport de certification

**ANSSI-CC-2019/46**

Nom du produit

**ST33TPHF20**

Référence/version du produit

**TPM Firmware 0x4A.0x40 & 0x4A.0x41**

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.4**

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



**SOG-IS**



**Ce certificat est reconnu au niveau EAL2  
augmenté de FLR.x.**

## 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
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> .....	7
1.2.4. <i>Identification du produit</i> .....	9
1.2.5. <i>Cycle de vie</i> .....	9
1.2.6. <i>Configuration évaluée</i> .....	9
<b>2. L’EVALUATION .....</b>	<b>10</b>
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
<b>3. LA CERTIFICATION .....</b>	<b>11</b>
3.1. CONCLUSION .....	11
3.2. RESTRICTIONS D’USAGE.....	11
3.3. RECONNAISSANCE DU CERTIFICAT .....	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	12
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>13</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>14</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>16</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le composant « ST33TPHF20, TPM Firmware 0x4A.0x40 & 0x4A.0x41 » développé par STMicroelectronics.

Ce produit est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs, etc.) conformément aux spécifications fonctionnelles TPM<sup>1</sup> 2.0. Le produit se décline sur une plateforme matérielle ST33HTPH en version A.C et le choix de la configuration du produit final (interface SPI<sup>2</sup> ou I<sup>2</sup>C<sup>3</sup>) est effectué au moment de la compilation du logiciel. La cible de sécurité [ST] décrit donc les deux versions possibles du produit.

## 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 s'inspire du 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 ;
- l'authentification de l'entité propriétaire ;
- 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 ;
- la gestion des registres de configuration (PCR<sup>4</sup>) ;
- la gestion de délégation et la gestion de la localité ;
- le stockage de la paire de clés EK<sup>5</sup> ;
- l'accès à des services cryptographiques dont les primitives sont supportées par la bibliothèque cryptographique NesLib 5.1.0 et par les modules cryptographiques matériels : AES 128 modes CTR et CFB, signature et chiffrement PKCS, MGF et dérivation de clé ;
- la génération de nombres aléatoires ;
- la signature RSA et ECDSA ;
- la destruction des valeurs de clés générées ;

---

<sup>1</sup> *Trusted Platform Module.*

<sup>2</sup> *Serial Peripheral Interface.*

<sup>3</sup> *Inter-Integrated Circuit.*

<sup>4</sup> *Platform Configuration Register.*

<sup>5</sup> *Endorsement Key.*



- la génération et la vérification des valeurs MAC (RSA, HMAC) et des HASH (SHA-1, SHA-256) ;
- la gestion des compteurs (*tick counters, monotonic counter*) ;
- la séquence de démarrage et l'autotest ;
- le 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 :

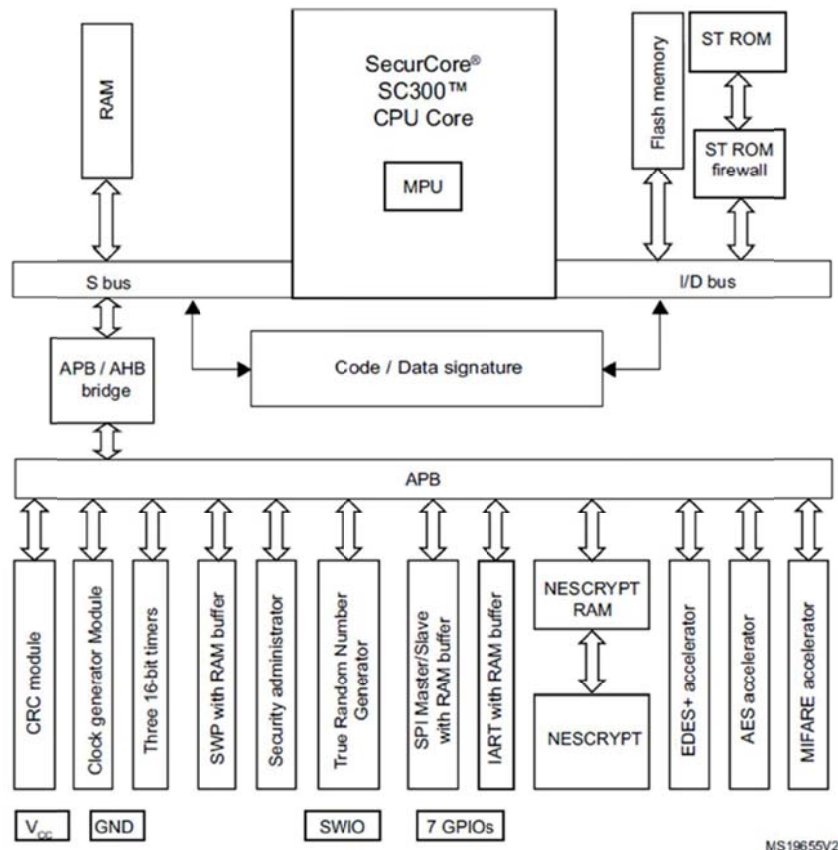


Figure 2 – Architecture matérielle

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 I<sup>2</sup>C ;
- de modules fonctionnels : compteurs, bloc de gestion d'interface série SPI ;
- de modules de sécurité : unité de protection des mémoires (MPU<sup>1</sup>), 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*), détection de fautes ;
- de coprocesseurs :
  - EDES pour le support des algorithmes DES ;
  - AES pour le support des algorithmes AES ;

<sup>1</sup> Memory Protection Uni.

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

L'architecture logicielle est la suivante :

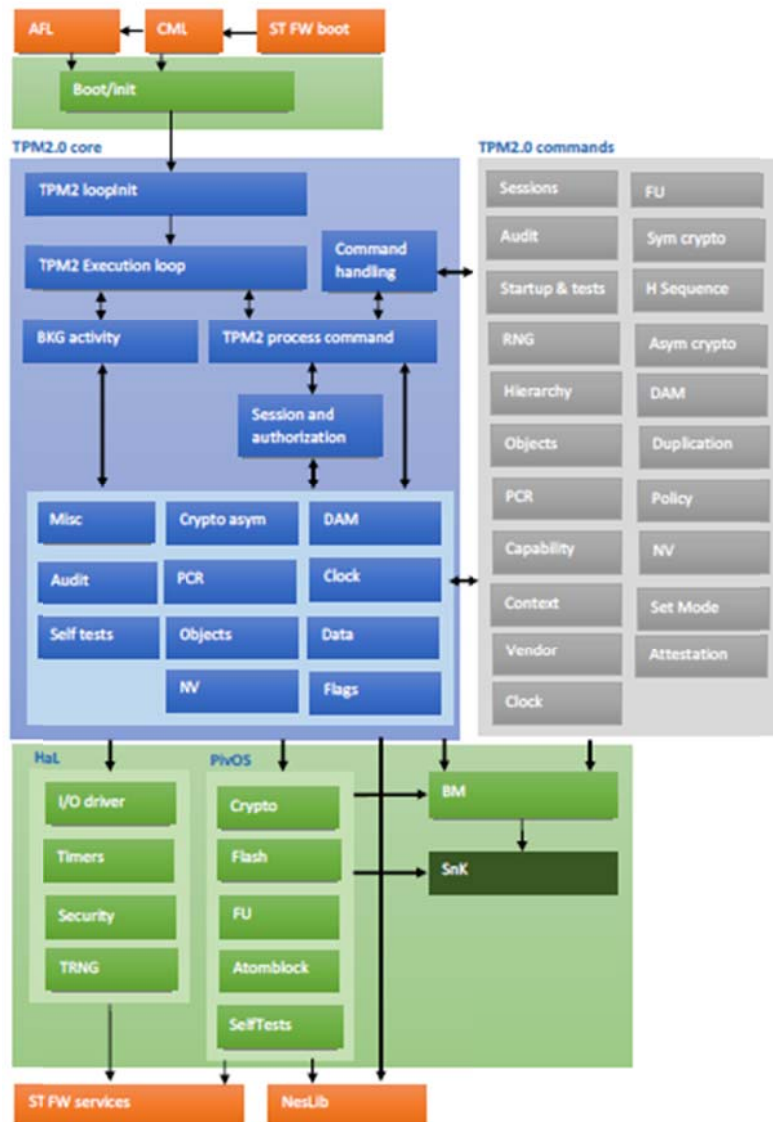


Figure 2 – Architecture logicielle

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

- le PivOS qui est un module supportant un ensemble de services de bas niveau ;
- la *Hardware Abstraction Layer* (HAL) qui est un ensemble de services fournis 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 module TPM 2.0 *core* ;
- le module TPM 2.0 *commands* ;
- la bibliothèque cryptographique NesLib version 5.1.0.

#### 1.2.4. Identification du produit

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

Les versions certifiées du produit sont identifiables en utilisant la commande « TPM\_GetCapability » afin d’obtenir les valeurs de « TPM\_CAP\_VERSION\_VAL » :

- soit pour I<sup>2</sup>C (version 0x4A 0x41), voir *Appendix A* et *Appendix B* du [GUIDE\_I2C] ;
- soit pour SPI (version 0x4A 0x40), voir *Appendix A* et *Appendix B* du [GUIDE\_SPI] suivant que le chargement du *firmware* est effectué en usine ou sur le terrain.

Pour connaître la version du produit, l’utilisateur peut également se référer au marquage inscrit sur le boîtier (voir [GUIDE\_I2C] §15 et [GUIDE\_SPI] §15 pour les références).

#### 1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST] §2.4).

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

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

#### 1.2.6. Configuration évaluée

Le certificat porte sur le composant « ST33TPHF20 mode TPM 2.0 firmware versions 0x4A.40 et 0x4A.41 », embarqué sur une plateforme matérielle ST33HTPH révision A en externe et C en interne, tel que présenté précédemment 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], 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 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 :

- 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 la référence [CER-2018/42] pour l'application TPM comme pour la bibliothèque cryptographique NesLib version 5.1.0 .

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 27 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.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 de produit [CER-2016/43]. 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 « ST33TPHF20, TPM Firmware 0x4A.0x40 & 0x4A.0x41 » 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.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<sup>1</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.org](http://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<sup>1</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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	1	1	Identification of security measures
	ALC_FLR				1				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	Advanced methodical 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"> <li>- ST33TPHF20 Mode TPM 2.0 TPM Firmware 0x4A.0x40 &amp; 0x4A.0x41 – Security Target, référence SSS_ST33TPHF20_M20_ST_18_001, version 04-00, daté du 15 juillet 2019, <i>STMICROELECTRONICS</i>.</li> </ul> <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"> <li>- ST33TPHF20 Mode TPM 2.0 TPM Firmware 0x4A.0x40 &amp; 0x4A.0x41 – Security Target Lite, référence SSS_ST33TPHF20_M20_STP_18_001, version 04-00p, daté du 15 septembre 2019, <i>STMICROELECTRONICS</i>.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report – SCAROLE-4A.40-4A-41, référence SCA_4A.40_4A.41_ETR, version 1.0, daté du 27 septembre 2019, <i>THALES/CNES</i>.</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- ST33TPHF20SPI – FW 0X4A.41 – HD1 – CONFIGURATION LIST, référence SSS_ST33TPHF20SPI_CFGL_19_001, version 01-00, daté du 11 septembre 2019, <i>STMICROELECTRONICS</i> ;</li> <li>- ST33TPHF20I2C – FW 0X4A.41 – HD3 – CONFIGURATION LIST, référence SSS_ST33TPHF20I2C_CFGL_19_001, version 01-00, daté du 11 septembre 2019, <i>STMICROELECTRONICS</i>.</li> </ul>
[GUIDES]	<ul style="list-style-type: none"> <li>- [GUIDE_I2C] : Datasheet – Flash-memory based TPM 2.0 device with an I<sup>2</sup>C interface, référence DS_ST33TPHF20I2C, version 4, daté du 10 septembre 2019, <i>STMICROELECTRONICS</i> ;</li> <li>- [GUIDE_SPI] : Datasheet – Flash memory-based TPM 2.0 device with an SPI interface, référence DS_ST33TPHF20SPI, version 11, daté du 12 septembre 2019, <i>STMICROELECTRONICS</i> ;</li> <li>- ST33TPHF20SPI Security recommendations, référence SSS_TPHF20_AN_16_001, version 01-02, daté du 27 octobre 2016, <i>STMICROELECTRONICS</i> ;</li> <li>- TPM EK certificate chip and EK authenticity verification, référence SSS_TPMEK_UM_15_001, version 02-00, daté du 11 mars 2016, <i>STMICROELECTRONICS</i>.</li> </ul>



[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> <li>- ALC Class Evaluation Report – C15P0036 Project, référence C15P0036_ALC_GEN_V2.0, version 2.0, daté du 11 juillet 2018, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- ALC Class Evaluation Report – C15P0036 Project, référence C15P0036_ALC_GEN_V1.0, version 1.0, daté du 2 juin 2018, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- ALC Class Evaluation Report – STM Project, référence STM_GEN_v2.0, version 2.0, daté du 21 décembre 2018, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- 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, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- Sites Visit Report Lite – STM AMK1, Loyang &amp; Calamba site audits, référence 17-0317-STM_SVR-M_v1.0, version 1.0, daté du 20 décembre 2017, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- Site Visit Lite Report – Toa Payoh site audit, référence 17-0317_TPY_SVR-M_v1.0, version 1.0, daté du 12 mars 2018, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- Site Visit Lite Report – STM CROLLES site audit, référence STM_Crolles_SVR-M_v1.0, version 1.0, daté du 18 juillet 2018, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- Site Audit Technical Report – STM Zaventem site audit, référence STM_Zaventem_STAR_v1.0, version 1.0, daté du 8 mars 2019, <i>SERMA SAFETY &amp; SECURITY</i> ;</li> <li>- Site Technical Audit Report – STM Rennes, référence STM_RNS_STAR_v1.0, version 1.0, daté du 22 mai 2019, <i>SERMA SAFETY &amp; SECURITY</i>.</li> </ul>
[PP-TPM]	<p>Profil de protection – PC Client Specific Trust Platform Module, TPM Library family 2.0, level 0, revision 1.38, version 1.1, daté du 10 aout 2018.  <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2018/03.</i></p>
[CER-2015/36]	<p>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 », 15/9/2015, ANSSI.</p>
[CER-2016/43]	<p>Rapport de certification ANSSI-CC-2016/43-M01 « ST33TPHF2ESPI mode TPM 2.0 TPM Firmware version 47.0C », daté du 16 février 2017, ANSSI.</p>
[CER-2018/42]	<p>Rapport de certification ANSSI-CC-2018/41 « ST33TPHF20 mode TPM 2.0, TPM Firmware versions 74.08 et 74.09 », daté du 24 septembre 2018, ANSSI.</p>

### 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 : <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;</li> <li>- Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;</li> <li>- Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI ( <i>Bundesamt für Sicherheit in der Informationstechnik</i> ).
[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.