



*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-2017/40**

### **ST33TPHF20I2C TPM Firmware version 74.05**

*Paris, le 19 juillet 2017*

*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.

<i>Référence du rapport de certification</i>	<b>ANSSI-CC-2017/40</b>
<i>Nom du produit</i>	<b>ST33TPHF20I2C</b>
<i>Référence/version du produit</i>	<b>Hardware ST33HTPH révision A/C (Externe/Interne), TPM Firmware 74.05</b>
<i>Conformité à un profil de protection</i>	<b>[PP-TPM] PC Client Specific Trusted Platform Module (Family 2.0, Level 0, Revision 1.16, version 1.0)</b>
<i>Critères d'évaluation et version</i>	<b>Critères Communs version 3.1 révision 4</b>
<i>Niveau d'évaluation</i>	<b>EAL 4 augmenté ALC_FLR.1, AVA_VAN.4</b>
<i>Développeur</i>	<b>STMicroelectronics Green Square Building B, Lambroekstraat, 5, B-1831 Diegem, Belgique</b>
<i>Commanditaire</i>	<b>STMicroelectronics Green Square Building B, Lambroekstraat,5, B-1831 Diegem, Belgique</b>
<i>Centre d'évaluation</i>	<b>THALES (TCS – CNES) 18 avenue Edouard Belin, BPI 1414, 31401 Toulouse Cedex 9, France</b>
<i>Accords de reconnaissance applicables</i>	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;"><b>CCRA</b> </div><div style="text-align: center;"><b>SOG-IS</b> </div></div> <p><b>Le produit est reconnu au niveau EAL2 augmenté d'ALC_FLR.1.</b></p>

# 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> .....	8
1.2.5. <i>Cycle de vie</i> .....	9
1.2.6. <i>Configuration évaluée</i> .....	10
<b>2. L’EVALUATION .....</b>	<b>11</b>
2.1. REFERENTIELS D’EVALUATION .....	11
2.2. TRAVAUX D’EVALUATION .....	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	11
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	11
2.5. CONCLUSION .....	12
2.6. RESTRICTIONS D’USAGE.....	12
2.7. RECONNAISSANCE DU CERTIFICAT .....	12
2.7.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	12
2.7.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	13
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>15</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>17</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le composant « ST33TPHF20I2C, hardware ST33HTPH révision A en externe et C en interne, TPM<sup>1</sup> firmware version 74.05<sup>2</sup> » 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<sup>3</sup> 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<sup>4</sup>) 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<sup>5</sup>) ;
- la gestion de délégation et la gestion de la localité ;
- le stockage de la paire de clés EK<sup>6</sup> ;
- la génération de clés et le stockage des clés (SRK<sup>7</sup>, *User Keys*, *PSS*<sup>8</sup>) ;
- 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 ;

---

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

<sup>2</sup> 4A.05 en hexadécimal.

<sup>3</sup> *Trusted Platform Module.*

<sup>4</sup> *Binary Large Object.*

<sup>5</sup> *Platform Configuration register.*

<sup>6</sup> *Endorsement Key.*

<sup>7</sup> *Storage Root Key.*

<sup>8</sup> *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 :

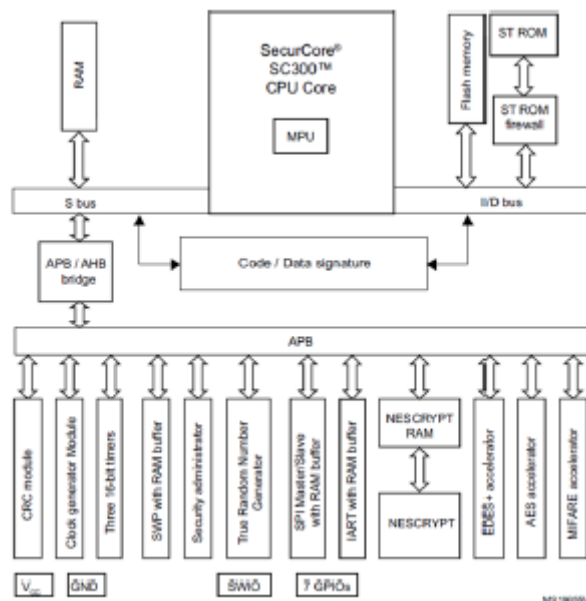


Figure 1 – Architecture *hardware*

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 I<sup>2</sup>C<sup>1</sup> ;
- de modules de sécurité : unité de protection des mémoires (MPU<sup>2</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 ;
  - NESCRIPT 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) ;

<sup>1</sup> Inter-Integrated Circuit.

<sup>2</sup> Memory Protection Unit.

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

A noter que par conception, cette plateforme *hardware* ne supporte pas le protocole I<sup>2</sup>C. Pour le rajouter, un *driver* compatible avec les spécifications [TCG] et [TCG Errata] a été implémenté. Le bus I<sup>2</sup>C est alors disponible via les ports « 7 GPIOx ».

L'architecture *firmware* est la suivante :

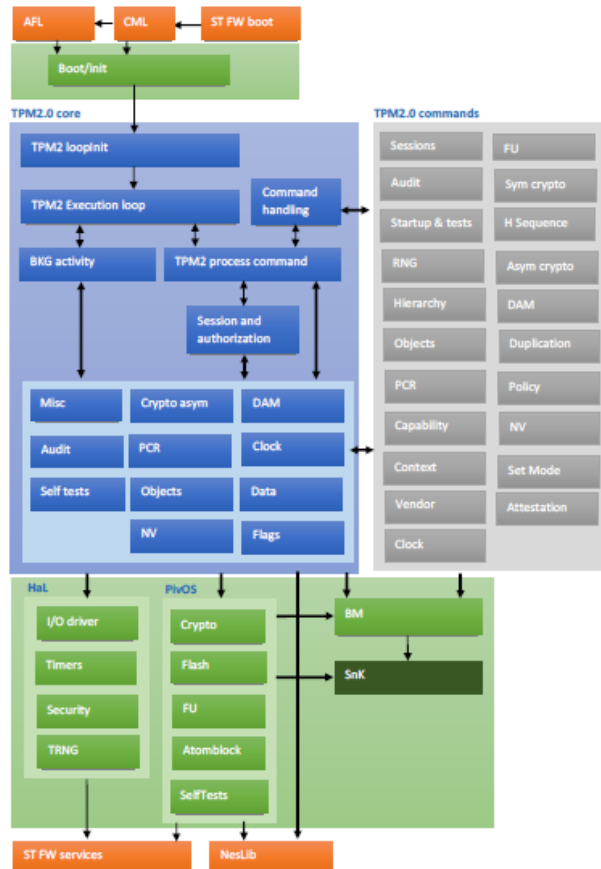


Figure 2 – Architecture *firmware*

La TOE *firmware* « F20 » est divisée en quatre blocs compilés :

- le TPM *firmware* qui est un bloc dynamique supportant les commandes TPM 2.0 ;
- l'*Application Flash Loader* qui est un bloc dynamique supportant la gestion du chargement de nouveaux *firmwares* ;
- le *Code Memory Loader* qui est un bloc statique responsable de vérifier l'intégrité des blocs dynamiques et démarrer l'un des blocs dynamiques quelle que soit la machine d'état du TPM ;
- la librairie cryptographique NesLib 5.1.0.

#### 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 [GUIDES]) :



- marquage externe « P68HAHB9 » (produit en mode TPM 2.0 uniquement) qui est la dénomination commerciale du composant ST33TPHF20I2C pour cette version de *firmware* ;
- informations inscrites sur la surface du composant :
  - *maskset reference* : K8K0 ;
  - *OST<sup>d</sup> revision (autotest ROM code)* : OST 2.2 (YQBF) ;
- contenu de « TMP\_CAP\_VENDOR\_PROPERTY » obtenu à partir de la commande « TMP2\_GetCapability » :
  - *hardware Chameleon code* : 48 42 39 00 (HB9) ;
  - *digest factory (32 bytes)* : EF 42 6F 9A 52 81 DF 11 49 55 69 92 92 4E 4D BC 3F FE DD F2 12 01 4B CC DF A6 A0 5D 07 2B CA C9 ;
  - *digest current (32 bytes)* : EF 42 6F 9A 52 81 DF 11 49 55 69 92 92 4E 4D BC 3F FE DD F2 12 01 4B CC DF A6 A0 5D 07 2B CA C9 ;
- contenu de « TMP\_CAP\_TPM\_PROPERTIES » obtenu à partir de la commande « TMP2\_GetCapability » :
  - *TPM firmware version* : 00 4A 00 05 ;
  - *internal firmware version* : 44 A0 11 63.

### 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 :

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

<sup>1</sup> *Operating System for Test.*

### ***1.2.6. Configuration évaluée***

Le certificat porte sur le composant « ST33TPHF20I2C, hardware ST33HTPH révision A en externe et C en interne, firmware version 74.05 », tel que présenté précédemment aux paragraphes 1.2.2, 1.2.3 et 1.2.4 et configuré conformément aux guides [GUIDES].

La librairie « Neslib 5.1 » et le *driver* I<sup>2</sup>C ont été évalués par le CESTI afin de :

- s'assurer que les recommandations de sécurité liées à l'I<sup>2</sup>C, soient respectées et correctement implémentées ;
- rechercher d'éventuelles vulnérabilités.

Le composant ST33TPHF20I2C 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-2016/43], [CER-2016/44] et [CER-2016/79].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 juin 2017, 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.

## 2.5. 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 « ST33TPHF20I2C, Hardware ST33HTPH révision A (externe) et C (interne), TPM Firmware version 74.05 » 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 et AVA\_VAN.4.

## 2.6. 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.

## 2.7. Reconnaissance du certificat

### 2.7.1. 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 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 :



---

<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).

### 2.7.2. *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
<b>ADV</b> 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
<b>AGD</b> 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
<b>ALC</b> 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	<b>Basic Flaw Remediation</b>
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
<b>ASE</b> 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
<b>ATE</b> 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
<b>AVA</b> Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	4	Moderate 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>- ST33TPHF20I2C TPM Firmware 0x4A 0x05, référence SSS_ST33TPHF20I2C_ST_17_001, version 01.00, 2 juin 2017, <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>- ST33TPHF20I2C TPM Firmware 0x4A.0X05, référence SSS-ST33TPHF20I2C_STP_17_001, version 01.00p, 2 juin 2017, <i>STMICROELECTRONICS</i>.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report – UGNI, référence UGN_ETR, version 1.0, 21 juin 2017, <i>THALES</i>.</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- TPM firmware F20 0x4A.0x05 for chip HB9 configuration list, référence SSS_TPMF20_HB9_CFGL_17_001, version 01-00, 2 juin 2017, <i>STMICROELECTRONICS</i>.</li> <li>- ST33HTPH rev C &amp; ST_Firmware rev1(ext) rev1(int) configuration list, référence SMD_33HTPM_HTPH_CFGL_16_001, version 01.01, <i>STMICROELECTRONICS</i>.</li> </ul>
[GUIDES]	<ul style="list-style-type: none"> <li>- Datasheet – Flash based TPM 2.0 device with an I2C interface, référence DS_ST33TPHF20I2C, version 1, mai 2017, <i>STMICROELECTRONICS</i>.</li> <li>- ST33TPMF2E – Security Guidelines for TPM Configuration, référence SSS_ST33TPMF2E_AN_15_005, version 01-03, 18 décembre 2015, <i>STMICROELECTRONICS</i>.</li> <li>- ST33TPHF2EI2C – FW 49.05, AGD deliveries, référence SSS_ST33TPHF2EI2C_4905_AGD_17_001, version 01-00, 26 mai 2017, <i>STMICROELECTRONICS</i>.</li> <li>- TPM EK certificate chip and EK authenticity verification, référence SSS_TPMEK_UM_15_001, version 02-00, 11 mars 2016, <i>STMICROELECTRONICS</i>.</li> <li>- ST33TPHF20SPI Security recommandations, référence SSS_TPHF20_AN_16_001, version 01-02, 27 octobre 2016, <i>STMICROELECTRONICS</i>.</li> </ul>
[PP-TPM]	<p>Profil de protection – PC Client Specific Trust Platform Module, family 2.0, level 0, revision 1.16, version 1.0, 6 mai 2015. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2015/07.</i></p>
[TCG]	<p>TPM I2C interface specification, family 2.0, level 00, revision 1.0, 7 octobre 2016, <i>TRUSTED COMPUTING GROUP</i>.</p>
[TCG Errata]	<p>Errata 1.0 for TCG TPM I2C interface specification, family 2.0, level 00, revision 1.0, 5 août 2016, <i>TRUSTED COMPUTING GROUP</i>.</p>

[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 », 15 septembre 2015, ANSSI.
[CER-2016/43]	Rapport de certification ANSSI-CC-2016/43 « ST33TPHF2ESPI mode TPM 2.0 TPM Firmware versions 47.00 et 47.04», 4 juillet 2016, ANSSI.
[CER-2016/44]	Rapport de certification ANSSI-CC-2016/44 « ST33TPHF2ESPI mode TPM 1.2, TPM Firmware versions 47.00 et 47.04 », 4 juillet 2016, ANSSI.
[CER-2016/79]	Rapport de certification ANSSI-CC-2015/80 du TPM « ST33TPHF20SPI, TPM Firmware version 74.00 (0x4A 0x00) », 13 décembre 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 ( <i>Bundesamt für Sicherheit in der Informationstechnik</i> ).
[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> .
[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.