PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2021/40

Trusted platform modules
ST33TPHF2X TPM FIRMWARE 1.512 & 2.512
ST33GTPMA/I TPM FIRMWARE 3.512 & 6.512

Paris, le 23 septembre 2021

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-2021/40

Nom du produit

Trusted platform modules ST33TPHF2X & ST33GTPMA/I

Référence/version du produit

ST33TPHF2X TPM FIRMWARE 1.512 & 2.512 and ST33GTPMA/I TPM FIRMWARE 3.512 & 6.512

Conformité à un profil de protection

Protection profile PC Client Specific TPM Level 0 Revision 1.38 Version 1.2

Critère 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 GRAND OUEST SAS

(Grand Ouest) SAS Rennes R&D
10, rue de Jouanet
35700 Rennes, France

Commanditaire

STMICROELECTRONICS GRAND OUEST SAS

(Grand Ouest) SAS Rennes R&D
10, rue de Jouanet
35700 Rennes, France

Centre d'évaluation

THALES / CNES

290 allée du Lac,
31670 Labège, France

Accords de reconnaissance applicables

CCRA

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

SOG-IS

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est la famille de TPM : « *Trusted platform modules ST33TPHF2X & ST33GTPMA/I, ST33TPHF2X TPM FIRMWARE 1.512 & 2.512 and ST33GTPMA/I TPM FIRMWARE 3.512 & 6.512* » développée par STMICROELECTRONICS GRAND OUEST SAS.

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 signatures et certificats, calcul de hachés et génération de nombres aléatoires) aux ordinateurs personnels, serveurs et imprimantes.

Les ST33GTPMA/I correspondent également à des gammes de *Trusted Platform Modules* et apportent des services similaires. Celle du ST33GTPMA est destinée au marché de l'automobile et celle du ST33GTPMI au marché industriel.

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 « PC Client Specific TPM/Level 0 revision 1.38 version 1.2 », voir [PP20].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits au chapitre « *2.2.1 TOE Usage and Security Features* » de la cible de sécurité [ST], tirés du [PP20].

1.2.3 *Architecture*

L'architecture du produit est décrite au chapitre « *2.3 TOE Description* » de la cible de sécurité. Pour les TPM ST33TPHF2X (respectivement ST33GTPMA/I), elle est principalement basée sur 5 sous-systèmes :

- le composant *Hardware* ST33HTPH (resp. ST33G1M2A ou ST33G1M2M) ;
- le *Firmware internal IC*: ST_Firmware rev 1 – YQBF (resp. rev1.3.2 – YYAF), incluant les *Flash drivers* ;
- le programme d'autotest dédié à la validation de la TOE en production : OST version 2.2 ;
- la librairie cryptographique NESLIB v6.5 ;
- le logiciel principal du TPM, incluant :
    - 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 ;
    - 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].

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST].

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES]-[CAPAB_PARAMS]. Les valeurs attendues pour chaque produit sont mentionnées dans leurs *datasheet* et *release manifest* respectifs, (voir [GUIDES]).

Les informations concernant l'IC (nommé *Harware commercial product* dans la table) sont données dans les documents [COF_HW_HTPH] et [CONF_HW_G1M2A0].

Eléments de configuration		Guides associés
Hardware commercial product ST33TPH *Maskset version* K8KA0 *External/Intern version* A/C	ST33TPHF2XSPI, Firmware version 1.512	[ST33TPHF2XSPI_DS] [SYREC]
	ST33TPHF2XSPI-C1, Firmware version 1.512	[ST33TPHF2XSPI-CI_DS] [SYREC]
	ST33TPHF2XI2C, Firmware version 2.512	[ST33TPHF2XI2C_DS] [SYREC]
Hardware commercial product ST33G1M2A *Maskset version* K8H0A *External/Intern version* F/G	ST33GTPMASPI, Firmware version 3.512	[ST33GTPMASPI_DS] [SYREC]
	ST33GTPMAI2C, Firmware version 6.512	[ST33GTPMAI2C_DS] [SYREC]
Hardware commercial product ST33G1M2M *Maskset version* K8H0A *External/Intern version* F/G	ST33GTPMISPI, Firmware version 3.512	[ST33GTPMISPI_DS] [SYREC]
	ST33GTPMII2C, Firmware version 6.512	[ST33GTPMII2C_DS] [SYREC]
Identification des logiciels embarqués	OST version 2.2	
	ST_Firmware rev 1 YQBF (pour ST33HTPH) ST_Firmware rev1.3.2 – YYAF (pour ST33G1M2A ou ST33G1M2M)	
Identification des bibliothèques	NESLIB version 6.5	

1.2.5 *Cycle de vie*

Le cycle de vie du produit correspond aux phases 1 et 2 du [PP20], comme rappelé dans la cible de sécurité [ST]. Le produit a été développé sur les sites suivants (voir [SITES]) :

STMicroelectronics ROUSSET Smartcard IC division 190, avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex, France	**STMicroelectronics ANG MO KIO** 18 Ang Mo Kio Industrial park 2, 569505 Singapour Singapour
STMicroelectronics RENNES 10, rue de Jouanet ePark 35700 Rennes	**STMicroelectronics ZAVENTEM** Green Square Lambroekstraat 5, Building B, 3rd floor

France	1831 Diegem/Machelen Belgium
STMicroelectronics CROLLES 850, rue Jean Monnet 38926 Crolles France	**STMicroelectronics TOA PAYOH** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour

1.2.6 *Configuration évaluée*

Le certificat porte sur :

- le composant « ST33TPHF2X » avec *hardware* ST33HTPH version A.C, *firmware* 1.512 (avec interface SPI) et 2.512 (avec interface I^2C) ;
- le composant « ST33GTPMA » avec *hardware* ST33G1M2A version F.G, *firmware* 3.512 (avec interface SPI) et 6.512 (avec interface I^2C) ;
- le composant « ST33GTPMI » avec *hardware* ST33G1M2A version F.G, *firmware* 3.512 (avec interface SPI) et 6.512 (avec interface I^2C),

tels que présentés aux paragraphes 1.2.2, 1.2.3 et 1.2.4 et configurés conformément aux guides [GUIDES].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie) détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01]] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto] lorsque les recommandations du guide [SCYREC] sont suivies. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01]. Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [ANSSI Crypto], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

Ce générateur d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31] et suivant les dispositions décrites dans la note d'application [CC-NOTE-24], montrant qu'il répondait aux exigences de la classe DRG.3.

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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2] , des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

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

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : *Trusted platform modules ST33TPHF2X TPM Firmawre 1.512 & 2.512 and ST33GTPMA/I TPM Firmware 3.512 & 6.512 security target*, référence SSS_ST33TPHF2X_GTPMA_GTPMI_ST_20_001, version 2.02, 27 juillet 2021. 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 Firmawre 1.512 & 2.512 and ST33GTPMA/I TPM Firmware 3.512 & 6.512 security target public*, référence ST33TPHF2X_GTPMAI_ST_0202p, version 2.02p, 27 juillet 2021.
[RTE]	Rapport technique d'évaluation : *Evaluation Technical Report, project CONDRIEU*, référence COND_ETR_v2.0, 18 août 2021.
[ANA-CRY]	*Analysis of Cryptographic Mechanisms, project CONDRIEU*, référence COND_Crypto_analysis_report_v1.0, 2 juillet 2021.
[CONF]	Liste de configuration du produit : • *ST33TPHF2X TPM FW 0X00.01.02.00 configuration list*, référence SSS_ST33TPHF2X_CFGL_21_001, version 01-01, 29 juin 2021 ; • *ST33TPHF2X TPM FW 0X00.02.02.00 configuration list, référence SSS_ST33TPHF2X_CFGL_21_002*, version 01-00, 20 janvier 2021 ; • *ST33GTPMA/ST33GTPMI TPM FW 0X00.03.02.00 configuration list,* référence SSS_ST33GTPMI_CFGL_21_001, version 01-00, 20 janvier 2021 ; • *ST33GTPMA/ST33GTPMI TPM FW 0X00.06.02.00 configuration list,* référence SSS_ST33GTPMI_CFGL_21_002, version 01-01, 29 juin 2021 ; • [CONF_LIST_HTPH] *Configuration List ST33HTPM and ST33HTPH rev C ST_Firmware rev 1 (ext)*, référence SMD_33HTPM_HTPH_CFGL_16_001, version 01.01, 15 juin 2021 ; • [CONF_LIST_G1M2A0] *ST33G1M2AM D01 Configuration List*, référence SMD_33H_CFGL_20_002, version 01.01, mars 2021.
[GUIDES]	*TCG TPM Main Specifications* : • *TPM Library Part1 Architecture Specification Family 2.0 rev 1.38 ;* • *TPM Library Part2 Structures Family 2.0 revision 1.38 ;* • *TPM Library Part3 Commands Family 2.0 revision 1.38 ;* • *TPM Library Part4 Supporting Routines Family 2.0 revision 1.38 ;* • *Errata for TPM Library Specification version 1.12 Family 2.0 revision 1.38*, *TCG PC-Client Specific Specifications* : • *TCG PC Client Platform TPM Profile (PTP) Specification,* référence family 2. level 00 revision 1.04, 3 février 2020 ; • *TCG EK Credential Profile For TPM Family 2.0; Level 0,* référence Specification Version 2.3 / Revision 2 - 23 juillet 2020,

	Specific Guidance documents (only one document apply according the protocol used) : • *ST33TPHF2XSPI datasheet* référence 17713_DS_ST33TPHF2XSPI_Rev-8, 4 mai 2021 ; • *ST33TPHF2XSPI-C1 datasheet*, référence 17747_DS_ST33TPHF2XSPI-C1_Rev-1, 11 juin 2021 ; • *ST33TPHF2XI2C datasheet,* référence 17734_DS_ST33TPHF2XI2C_Rev-4, 12 mai 2021 ; • *ST33GTPMASPI datasheet,* référence 17756_DS_ST33GTPMASPI_Rev-4, 11 juin 2021 ; • *ST33GTPMAI2C datasheet,* référence 17790_DS_ST33GTPMAI2C_Rev-6, 10 juin 2021 ; • *ST33GTPMISPI datasheet,* référence 17755_DS_ST33GTPMISPI_Rev-2, 11 juin 2021 ; • *ST33GTPMII2C datasheet,* référence 17754_DS_ST33GTPMII2C_Rev-2, 11 juin 2021, *Specific preparative document* • [SCYREC] *ST33TPHF2X, ST33GTPMA, ST33GTPMI - Security recommendations,* référence SSS_ST33TPHFX_AN_21_001, version 2-00, 8 mars 2021.
[SITES]	• *ALC_GEN 2020/2021 : ALC Class Evaluation Report STM_2020_V2 Project*, référence STM_2020_V2_GEN_v1.0, 08/07/2020 ; • *ST ROUSSET, Site Technical Audit Report – STM Rousset*, référence STM2020_RST_STAR_v1.1, 8/12/2020 ; • *ST Rennes, Site Technical Audit Report STMicroelectronics Rennes*, référence STM_2020_V2_RNS_STAR_v1.0, 15/03/2021 ; • *ST Ang Mo Kio (Singapore), Site Technical Audit Report - Ang Mo Kio 1 Site Audit*, référence STM2020_AMK1_STAR_V1.1, 15/06/2020 ; • *ST Zaventem (Belgium), STMicroelectronics Development Environment ST Zaventem, Site Technical Audit Report*, référence STM2020-v2_ZVT_STAR_v1.0, 29/03/2021 ; • *ST Crolles, Site Technical Audit Report - STM Crolles site audit*, référence STM2020_CRL_STAR_v1,0, 13 octobre 2020 ; • *ST Toa Payoh, Site Technical Audit Report TPY and AMK 6*, référence STM2020_TPY-AMK6_STAR_v1.0, 24/02/2020.
[PP20]	*Protection Profile PC Client Specific TPM, TPM Library specification Family « 2.0 », Level 0, revision 1.38 version 1.2*, certifié sous la référence ANSSI-CC-PP-2020/01 le 9 juin 2020.

ANNEXE B. 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.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, 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 and similar devices*, version 3.1, juin 2020.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[AIS20/31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[CC-NOTE-24]	NOTE D'APPLICATION : EVALUATIONS DE GENERATEURS D'ALEA SELON AIS20/31 DANS LE SCHEMA FRANÇAIS, référence ANSSI-CC-NOTE-24_1.0, 2 mars 2021.

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