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-2025/10

ST33KTPM2XSPI & ST33KTPM2X (TPM FIRMWARE 9.512)

Paris, le 07 Mars 2025

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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

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 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.cyber.gouv.fr.

TABLE DES MATIERES

1 Résumé

Référence du rapport de certification **ANSSI-CC-2025/10**
Nom du produit **ST33KTPM2XSPI & ST33KTPM2X**
Référence/version du produit **TPM FIRMWARE 9.512**
Type de produit **Cartes à puce et dispositifs similaires**
Conformité à un profil de protection ***Protection Profile PC Client Specific TPM*** *PP PCCS TPM F2.0 L0 r1.59 V1.3, certifié ANSSI-CC-PP-2021/02 le 30 novembre 2021*
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL4 augmenté** ALC_DVS.2, ALC_FLR.1, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report CHINOOK1 / ST33KTPM2XSPI & ST33KTPM2X / TPM FW 9.512*, référence CHN1_ETR, Version 3.0, 14 février 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Exigences de configuration du produit voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage
Développeur **STMICROELECTRONICS** 10 rue de Jouanet, 35700 Rennes, France
Commanditaire **STMICROELECTRONICS** 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 ALC_FLR.1.

SOG-IS

2 Le produit

2.1 Présentation du produit

Le produit évalué est « ST33KTPM2XSPI & ST33KTPM2X, TPM FIRMWARE 9.512 » développé par STMICROELECTRONICS.

Ce produit est un TPM (*Trusted Platform Module*). Il est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs, etc.) conformément aux spécifications fonctionnelles TPM2.0.

2.2 Description du produit

2.2.1 *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].

2.2.2 *Services de sécurité*

Les services de sécurité évalués fournis par le produit sont présentés au chapitre 2.2.1 « *TOE Usage and Security Features »* de la cible de sécurité [ST].

2.2.3 *Architecture*

Ce produit peut être décomposé en deux parties distinctes : une partie logicielle et une partie matérielle.

Le produit est constitué des composants présentés au chapitre 2.3 *« TOE Description »* de la cible de sécurité [ST].

2.2.4 *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 1 de la cible de sécurité [ST] au chapitre 2.1 « *TOE identification* ».

2.2.5 *Cycle de vie*

Le cycle de vie du produit suit les phases décrites dans [PP-TPM] et les sites impliqués sont précisés dans le chapitre 2.4 « *TOE lifecycle* » de la cible de sécurité [ST].

2.2.6 *Configuration évaluée*

Le certificat porte sur les configurations permises par la cible de sécurité [ST].

3 L'évaluation

3.1 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 et dispositifs similaires, 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).

3.2 Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « ST33K1M5T », voir [CER_IC].

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

3.3 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 a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

3.4 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.

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER_IC]).

Par ailleurs, comme requis dans le référentiel [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

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.

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2025/10, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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].

4.3 Reconnaissance du certificat

4.3.1 *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 :

4.3.2 *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 ST33KTPM2XSPI & ST33KTPM2X TPM FIRMWARE 9.512,* référence SMD_ST33KTPM2X_ST_21_001, version 2.3, 6 février 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *TRUSTED PLATFORM MODULES ST33KTPM2XSPI & ST33KTPM2X TPM FIRMWARE 9.512,* référence SMD_ST33KTPM2X_ST_21_001, version 2.3p, 6 février 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report CHINOOK1 / ST33KTPM2XSPI & ST33KTPM2X / TPM FW 9.512*, référence CHN1_ETR, version 3.0, 14 février 2025.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms CHINOOK2*, référence CHN2_CRY, version 3.0, 5 décembre 2024.
[CONF]	Liste de configuration du produit : *ST33KTPM2X FW 9.512 CONFIGURATION LIST*, référence SSS_ST33KTPM2X_CFGL_24_002, version 1.2, 6 février 2025.
[GUIDES]	- *Trusted Platform Module Library Part 1: Architecture*, révision 1.59, 8 novembre 2019. - *Trusted Platform Module Library Part 1: Structures*, révision 1.59, 8 novembre 2019. - *Trusted Platform Module Library Part 1: Commands*, révision 1.59, 8 novembre 2019. - *Trusted Platform Module Library Part 1: Supporting Routines*, révision 1.59, 8 novembre 2019. - *Errata for TCG Trusted Platform Module Library*, version 1.5, 9 janvier 2024. - *TCG PC Client Platform TPM Profile Specification for TPM 2.0*, version 1.05, 4 septembre 2020. - *Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14*, version 1.0, 4 septembre 2020. - *TCG EK Credential Profile For TPM Family 2.0; Level 0*, version 2.3, 23 juillet 2020. - *ST33KTPM2XSPI Datasheet: STSAFE-TPM trusted platform module 2.0 with a SPI interface*, référence DS_ST33KTPM2XSPI, version 14, décembre 2024. - *ST33KTPM2X Datasheet STSAFE-TPM trusted platform module 2.0 with a SPI or I^2C interface*, référence DS_ST33KTPM2X, version 4, décembre 2024.

	- *ST33KTPM2X - Security recommendations*, référence SSS_ST33KTPM2X_AN_22_001, version 1.6, 25 octobre 2024.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - STM_2024_ALC_GEN_v1.1 ; - STM_2022_RNS_STAR_v1.1 ; - STM_2024_ST Zaventem_STAR_v1.0 ; - STM_2024_ST_Crolles_STAR_v1.0 ; - STM_2023_RST_CMP_STAR_v1.2 ; - STM_2023_TPY-AMK6_STAR_v1.0.
[CER_IC]	Produit « ST33K1M5C and ST33K1M5T » Certifié par le NSCIB sous la référence NSCIB-CC-2300056-02 le 26 septembre 2024.
[PP-TPM]	*Protection Profile PC Client Specific TPM*, PP PCCS TPM F2.0 L0 r1.59 V1.3, certifié ANSSI-CC-PP-2021/02 le 30 novembre 2021.

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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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 3.2.1, février 2024.
[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.

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