



**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-2024/04

Trusted Platform Modules ST33KTPM2XSPI & ST33KTPM2X (TPM Firmware 9.257)

Paris, le 04 Avril 2024

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

Vincent STRUBEL

[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

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

Référence du rapport de certification	ANSSI-CC-2024/04
Nom du produit	Trusted Platform Modules ST33KTPM2XSPI & ST33KTPM2X
Référence/version du produit	TPM Firmware 9.257
Conformité à un profil de protection	Protection Profile PC Client Specific TPM PP PCCS TPM F2.0 LO r1.59 V1.3, certifié ANSSI-CC-PP-2021/02 le 30 novembre 2021 avec conformité aux packages : "ECDAAs Optional Package"
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
Développeur	STMICROELECTRONICS GRAND OUEST SAS 10 rue de Jouanet, 35700, Rennes, France
Commanditaire	STMICROELECTRONICS GRAND OUEST SAS 10 rue de Jouanet, 35700, Rennes, France
Centre d'évaluation	THALES / CNES 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables	  Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.1.

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.cyber.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit.....	6
1.2.1	Introduction	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture	6
1.2.4	Identification du produit.....	6
1.2.5	Cycle de vie	6
1.2.6	Configuration évaluée	6
2	L'évaluation.....	7
2.1	Référentiels d'évaluation	7
2.2	Travaux d'évaluation	7
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	8
2.4	Analyse du générateur d'aléa.....	8
3	La certification	9
3.1	Conclusion.....	9
3.2	Restrictions d'usage	9
3.3	Reconnaissance du certificat.....	10
3.3.1	Reconnaissance européenne (SOG-IS).....	10
3.3.2	Reconnaissance internationale critères communs (CCRA).....	10
ANNEXE A.	Références documentaires du produit évalué	11
ANNEXE B.	Références liées à la certification	12

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Trusted Platform Modules ST33KTPM2XSPI & ST33KTPM2X, TPM Firmware 9.257 » développé par STMICROELECTRONICS GRAND OUEST SAS.

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.) en implémentant les spécifications fonctionnelles TPM2.0.

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 décrits au chapitre 2.2.1 « *TOE Usage and Security Features* » de la cible de sécurité [ST].

1.2.3 Architecture

L'architecture du produit est décrite au chapitre 2.3 « *TOE Description* » de la cible de sécurité [ST].

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 la valeur *TPM embedded software Version Major.Minor* indiquée dans la cible de sécurité [ST] au chapitre 2.1 « *TOE identification* » dans la table 1 « *Target of evaluation reference* ». Cette valeur peut être vérifiée par une commande spécifiée dans les [GUIDES].

1.2.5 Cycle de vie

Le cycle de vie du produit est décrit au chapitre 2.4 « *TOE lifecycle* » de la cible de sécurité [ST] ; les noms des [SITES] de développement et de fabrication y sont indiqués.

1.2.6 Configuration évaluée

Le certificat porte sur les configurations permises par la cible de sécurité [ST], lorsque les guides sont appliqués.

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

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 « *ST33K1M5C and ST33K1M5T C01* », voir [CER_IC], et de leur bibliothèque « *Cryptographic library NesLib 6.7.4 on ST33K1M5C and ST33K1M5T C01* », voir [CER_LIB].

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** ».

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 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.

2.4 Analyse du générateur d'aléa

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.

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'accord¹, 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 signataires², 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]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none">- <i>TRUSTED PLATFORM MODULES ST33KTPM2XSPI & ST33KTPM2X TPM FIRMWARE 9.257 SECURITY TARGET</i>, référence <i>SMD_ST33KTPM2X_ST_21_001</i>, version 01.04, 5 janvier 2024. <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">- <i>TRUSTED PLATFORM MODULES ST33KTPM2XSPI & ST33KTPM2X TPM FIRMWARE 9.257 SECURITY TARGET</i>, référence <i>SMD_ST33KTPM2X_ST_21_001</i>, version 01.04p, 5 janvier 2024.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- <i>Evaluation Technical Report CITRA1 / ST33KTPM2XSPI & ST33KTPM2X / TPM FIRMWARE 9.257</i>, référence <i>CITRA1_ETR</i>, version 1.1, 27 février 2024.
[ANA_CRY]	<p><i>Analysis of Cryptographic Mechanisms CITRA</i>, référence <i>CITRA_CRY_v1.0</i>, version 1.0, 24 octobre 2023.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none">- <i>ST33KTPM2X TPM FW 0x00.09.01.01 CONFIGURATION LIST</i>, référence <i>SSS_ST33KTPM2X_CFGL_23_001</i>, 18 janvier 2024.
[GUIDES]	<p>La table 2 de la cible de sécurité [ST] indique les guides du produit. Cette table donne pour chaque guide l'indication de sa version et de sa date de parution</p>
[SITES]	<p>Références des rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none">- <i>STM_2023_ALC_GEN_v1.1</i> ;- <i>STM_2022_RNS_STAR_v1.1</i> ;- <i>STM_2021_RST_STAR_v1.1</i> ;- <i>STM-2021_TPY-AMK6_STAR_v1.0</i> ;
[CER_IC]	<p>Certification Report <i>ST33K1M5C and ST33K1M5T C01</i>, NSCIB-CC-2300056-01-CR, 10 août 2023.</p>
[CER_LIB]	<p>Certification Report <i>NesLib 6.7.4 on ST33K1M5C and ST33K1M5T C01</i>, NSCIB-CC-2300114-01-CR, 18 décembre 2023.</p>
[PP-TPM]	<p><i>Protection Profile PC Client Specific TPM</i>, PP PCCS TPM F2.0 L0 r1.59 V1.3, certifié ANSSI-CC-PP-2021/02 le 30 novembre 2021.</p>

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, les sites 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-P-01, version 4.1.
[CC]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none">- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2, novembre 2022.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , 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.