PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de maintenance
ANSSI-CC-2024/04-M01

ST33KTPM2XSPI

(TPM Firmware 9.258)

Certificat de référence : ANSSI-CC-2024/04

Paris le 02 Septembre 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

AVERTISSEMENT

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

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

1 Références

[CER]	Rapport de certification ANSSI-CC-2024/04, Trusted Platform Modules ST33KTPM2XSPI & ST33KTPM2X, TPM Firmware 9.257, 4 avril 2024.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	ST33KTPM2X FW 00.09.01.02 Security Impact Analysis Report, SSS_ST33KTPM2X_SIA_24_001 version 01.00, 8 janvier 2024, STMICROELECTRONICS.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.*
[CCRA]	*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.*

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « ST33KTPM2XSPI, (TPM Firmware 9.258) » développé par la société STMICROELECTRONICS.

Le produit a été initialement certifié sous la référence ANSSI-CC-2024/04 (référence [CER]).

La version maintenue du produit est identifiable par la valeur 9.258 assignée à *« TPM embedded software version major.minor »*.

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- Correction de bugs ;
- Support de la taille 3072bits pour la clef RSA *Endorsment Key* et son certificat.

4 Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	*TPM Library Part 1*: Architecture, Specification Version 2.0, Revision 1.59.	[CER]
	TPM Library Part 2: Architecture, Specification Version 2.0, Revision 1.59.	[CER]
	TPM Library Part 3: Architecture, Specification Version 2.0, Revision 1.59.	[CER]
	TPM Library Part 4: Architecture, Specification Version 2.0, Revision 1.59.	[CER]
	Errata version 1.4 *for TCG TPM library version* 2.0 revision 1.59.	[CER]
	TCG PC Client Specific Platform TPM Profile for TPM 2.0 (PTP), Family "2.0", Version 1.05 revision 14.	[CER]
	Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14 – version 1.0.	[CER]
	TCG EK credential profile for TPM Family 2.0 Level 0. Specification Version 2.3.	[CER]
	ST33KTPM2XSPI datasheet: STSAFE-TPM trusted platform module 2.0 with a SPI interface, version 8, 8 décembre 2023.	[CER] *(only for firmware 9.257)*
	ST33KTPM2X Datasheet STSAFE-TPM trusted platform module 2.0 with a SPI or I²C interface, version 3, 15 décembre 2023.	[CER]
	ST33KTPM2XSPI datasheet: STSAFE-TPM trusted platform module 2.0 with a SPI interface, version 12, 1er mars 2024.	[R-M01]
	ST33KTPM2X - Security recommendations.	[CER]
[ST]	*Trusted Platform Modules ST33KTPM2XSPI & ST33KTPM2X TPM Firmware 9.257 & ST33KTPM2XSPI TPM Firmware 9.258, Security Target,* référence SMC_ST33KTPM2X_ST_21_0001, version 01.05, 27 mars 2024. Version publique : *Trusted Platform Modules ST33KTPM2XSPI & ST33KTPM2X TPM Firmware 9.257 & ST33KTPM2XSPI TPM Firmware 9.258, Security Target,* référence SMC_ST33KTPM2X_ST_21_0001, version 01.05p, 24 mai 2024.	[R-M01]
[CONF]	*ST33KTPM2X – TPM Firmware 9.258 configuraiton list*, référence SSS_ST33KTPM2X_CFGL_24_001, version 01.01 , 16 mai 2024.	[R-M01]

5 Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur.

Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

6 Reconnaissance du certificat

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 :

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.

[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.