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 maintenance ANSSI-CC-2019/37-M02

ST33TPHF2X with TPM Firmware 1.256, 1.257, 1.258 & 2.256, 2.272

ST33GTPMA with TPM Firmware 3.256 & 6.256

Certificat de référence : ANSSI-CC-2019/37

Paris, le 1er avril 2020

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2019/37 du produit ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTPMA with TPM Firmware 3.256 & 6.256, certifié le 18 octobre par l'ANSSI.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2019/37-M01, ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTPMA with TPM Firmware 3.256 & 6.256.
[IAR]	ST33TPHF2XSPI SECURITY IMPACT ANALYSIS REPORT FW 1.258 vs 1.257, référence SSS_ST33TPHF2XSPI_SIA_20_002, daté du 3 mars 2020, *STMICROELECTRONICS* ; ST33TPHF2XI2C SECURITY IMPACT ANALYSIS REPORT FW 2.272 vs 2.256, référence SSS_ST33TPHF2X_SIA_20_001, daté du 2 janvier 2020, *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 ST33TPHF2X with TPM Firmware 1.256, 1.257, 1.258 & 2.256, 2.272, ST33GTPMA with TPM Firmware 3.256 & 6.256 développé par la société *STMICROELECTRONICS*.

Le produit « ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTMPA with TPM Firmware 3.256 & 6.256 » a été initialement certifié sous la référence ANSSI-CC-2019/37 (référence [CER]).

Il a déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2019/37-M01 (référence [R-M01]).

La version maintenue du produit est identifiable en utilisant la commande « TPM2_GetCapability » afin d'obtenir les valeurs de « TPM_CAP_VENDOR_PROPERTY » :

- Pour ST33TPHF2X :
  - avec interface SPI et *firmware* 1.258, voir *Appendix* A de [DS_1.258] ;
  - avec interface I2C et *firmware* 2.272, voir *Appendix* A de [DS_2.272].

3. Description des évolutions

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

- résolution d'un problème de latence lors de la mise à jour de registre ainsi que des effets liés à ce correctif ;
- résolution d'un problème d'*offset* apparu dans le code assembleur ;
- résolution d'un problème de *timing* pour se conformer à la spécification du protocole I2C ;
- correction de la gestion d'interruption GPIO *reset* dans la communication I2C ;
- résolution d'un conflit de bus I2C.

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-M02] référence la présente maintenance.

Les guides contenant de nouvelles recommandations sécuritaires obligatoires par rapport au certificat initial apparaissent en gras.

[GUIDES]	[DS_1.256] ST33TPHF2XSPI Datasheet – Production data : Flash-memory-based TPM 2.0 device with an SPI interface and extended features, référence DS_ST33TPHF2XSPI Rev 2, version 2, daté du 17 avril 2019, *STMICROELECTRONICS.*	[CER]
	[DS_1.257] ST33TPHF2XSPI Datasheet – Production data : Flash-memory-based TPM 2.0 device with an SPI interface and extended features, référence DS_ST33TPHF2XSPI Rev 3, version 3, daté du 24 juillet 2019, *STMICROELECTRONICS.*	[CER]
	[DS_1.258] ST33TPHF2XSPI Datasheet – Production data : Flash-memory-based TPM 2.0 device with an SPI interface and extended features, référence DS_ST33TPHF2XSPI Rev 4, version 4, daté du 13 mars 2020, *STMICROELECTRONICS.*	[R-M02]
	[DS_2.256] ST33TPHF2XI2C Datasheet – Production data : Long-term evolution TPM 2.0 device with an I²C interface, référence DS_ST33TPHF2XI2C Rev 1, version 1, daté du 5 juillet 2019, *STMICROELECTRONICS.*	[CER]
	[DS_2.272] ST33TPHF2XI2C Datasheet – Production data : Long-term evolution TPM 2.0 device with an I²C interface, référence DS_ST33TPHF2XI2C Rev 2, version 2, daté du 7 février 2020, *STMICROELECTRONICS.*	[R-M02]
	[DS_3.256] ST33GTPMASPI Datasheet – Production data : Flash-memory-based TPM 2.0 device for automative applications with an SPI interface , référence DS_ST33GTPMASPI Rev 3, version 3, daté du 25 juillet 2019, *STMICROELECTRONICS.*	[CER]
	[DS_6.256] ST33GTPMAI2C Datasheet – Production data : Flash-memory-based TPM 2.0 device for automative applications with an I²C interface ,	[CER]

	référence DS_ST33GTPMAI2C Rev 3, version 3, daté du 26 juillet 2019, *STMICROELECTRONICS*.	
	TPM EK Certificate – Chip and EK authenticity verification, référence SSS_TPMEK_UM_15_001, version 2, daté du 11 mars 2016, *STMICROELECTRONICS*.	[CER]
	ST33TPHF20SPI – Security recommendations, référence SSS_TPHF20_AN_16_001, version 1.2, daté du 27 octobre 2016, *STMICROELECTRONICS*.	[CER]
[ST]	Cibles de sécurité de référence : - Trusted platforms modules ST33TPHF2X TPM firmware 1.256, 1.257, 1.258 & 2.256, 2.272 and ST33GTPMA TPM firmware 3.256 & 6.256 Security Target, référence SSS_ST33TPHF2X_GTPMA_ST_18_001, version 1.2, daté du 6 mars 2020, *STMICROELECTRONICS*. Version publique : - Trusted platforms modules ST33TPHF2X TPM firmware 1.256, 1.257, 1.258 & 2.256, 2.272 and ST33GTPMA TPM firmware 3.256 & 6.256 Security Target, référence SSS_ST33TPHF2X_GTPMA_ST_18_001 public, version 1.2p, daté du 6 mars 2020, *STMICROELECTRONICS*.	[R-M02]
[CONF]	TPM FIRMWARE F2X 00.01.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HC4_CFGL_19_001, version 1, daté du 21 juin 2019, *STMICROELECTRONICS*.	[CER]
	TPM FIRMWARE F2X HC5 00.02.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HC5_CFGL_19_001, version 1, daté du 5 juillet 2019, *STMICROELECTRONICS*.	[CER]
	TPM FIRMWARE F2X HD8 00.01.01.02 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HD8_CFGL_20_001, version 1, daté du 19 mars 2020, *STMICROELECTRONICS*.	[R-M02]
	TPM FIRMWARE F2X HD4 00.01.01.01 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HD4_CFGL_19_001, version 1, daté du 27 juin 2019, *STMICROELECTRONICS*.	[CER]
	TPM FIRMWARE F2X HD5 00.02.01.10 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_HD5_CFGL_20_001, version 1, daté du 4 mars 2020, *STMICROELECTRONICS*.	[R-M02]
	TPM FIRMWARE F2X AE5 00.03.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_AE5_CFGL_19_001, version 1, daté du 25 juin 2019, *STMICROELECTRONICS*.	[CER]

	TPM FIRMWARE F2X AE6 00.06.01.00 – CONFIGURATION LIST, référence SSS_ST33TPHF2X_AE6_CFGL_19_001, version 1, daté du 26 juin 2019, *STMICROELECTRONICS*.	[CER]

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

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été 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.org.

2 Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.