



**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 maintenance ANSSI-CC-2019/37-M03**

**ST33TPHF2X with TPM Firmware 1.256,  
1.257, 1.258 & 2.256, 2.272  
ST33GTPMA/I with TPM Firmware 3.256,  
3.257 & 6.256, 6.257**

**Certificat de référence : ANSSI-CC-2019/37**

Paris, le 30 novembre 2020

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

Guillaume POUPARD

[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](mailto:certification@ssi.gouv.fr)

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

## 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 2019 par l'ANSSI.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[R-M02]	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, daté du 1 <sup>er</sup> avril 2020.
[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, daté du 16 décembre 2019.
[IAR]	ST33GTPMI SECURITY IMPACT ANALYSIS REPORT FW 6.257 VS. 6.256 and 3.257 VS. 3.256, référence SSS_ST33GTPMI_SIA_20_031, daté du 15 mai 2020.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</i>
[CCRA]	<i>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.</i>

## 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 and ST33GTPMA/I with TPM Firmware 3.256, 3.257 & 6.256, 6.257 » développé par la société STMicroelectronics.

Le produit « ST33TPHF2X with TPM Firmware 1.256, 1.257 & 2.256, ST33GTPMA 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 de deux maintenances sous les références ANSSI-CC-2019/37-M01 (référence [R-M01]) et ANSSI-CC-2019/37-M02 (référence [R-M02]).

La version maintenue du produit est identifiable en utilisant la commande « TPM2\_GetCapability » afin d'obtenir les valeurs de « TPM\_CAP\_VENDOR\_PROPERTY » :

- Pour ST33GTPMA/I :
  - o avec interface SPI et *firmware* version 3.257, voir *Appendix A* de [DS\_3.257] ;
  - o avec interface I2C et *firmware* version 6.257, voir *Appendix A* de [DS\_6.257].

## 3 Description des évolutions

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

- corrections d'écart à la norme I2C ;
- corrections de gestion du *reset* lors des communications en I2C ;

- correction d'un conflit de bus I2C.

Par ailleurs les nouvelles versions des bibliothèques TPM 3.257 et 6.257 sont embarquées sur le microcontrôleur ST33G1M2M plutôt que ST33G1M2A. Ce changement induit une modification du nom de produit ST33GTPMI plutôt que ST33GTPMA. Les produits sont en fait identiques, le changement de dénomination du microcontrôleur (qui implique celui du produit maintenu) n'est dû qu'à une exigence plus grande lors des tests de performance lors de la phase de production.

#### 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-M03] référence la présente maintenance.

[GUIDES]	<i>[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.</i>	[CER]
	<i>[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.</i>	[CER]
	<i>[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.</i>	[R-M02]
	<i>[DS_2.256] ST33TPHF2XI2C Datasheet – Production data : Long-term evolution TPM 2.0 device with an I<sup>2</sup>C interface, référence DS_ST33TPHF2XI2C Rev 1, version 1, daté du 5 juillet 2019, STMicroelectronics.</i>	[CER]
	<i>[DS_2.272] ST33TPHF2XI2C Datasheet – Production data : Long-term evolution TPM 2.0 device with an I<sup>2</sup>C interface, référence DS_ST33TPHF2XI2C Rev 2, version 2, daté du 7 février 2020, STMicroelectronics.</i>	[R-M02]
	<i>[DS_3.256] ST33GTPMASPI Datasheet – Production data : Flash-memory-based TPM 2.0 device for automotive applications with an SPI interface, référence DS_ST33GTPMASPI Rev 3, version 3, daté du 25 juillet 2019, STMicroelectronics.</i>	[CER]
	<i>[DS_6.256] ST33GTPMAI2C Datasheet – Production data : Flash-memory-based TPM 2.0 device for automotive applications with an I<sup>2</sup>C interface, référence DS_ST33GTPMAI2C Rev 3, version 3, daté du 26 juillet 2019, STMicroelectronics.</i>	[CER]
	<i>[DS_3.257] ST33GTPMISPI Datasheet – Production data : Flash-memory-based TPM 2.0 device for industrial applications with an SPI interface, référence DS_ST33GTPMISPI Rev 1, version 1, daté du 18 septembre 2020, STMicroelectronics.</i>	[R-M03]

	<i>[DS_6.257] ST33GTPMII2C Datasheet – Production data : Flash-memory-based TPM 2.0 device for industrial applications with an I<sup>2</sup>C interface, référence DS_ST33GTPMII2C Rev 1, version 1, daté du 18 septembre 2020, STMicroelectronics.</i>	[R-M03]
	<i>TPM EK Certificate – Chip and EK authenticity verification, référence SSS_TPMEK_UM_15_001, version 2, daté du 11 mars 2016, STMicroelectronics.</i>	[CER]
	<i>ST33TPHF20SPI – Security recommendations, référence SSS_TPHF20_AN_16_001, version 1.2, daté du 27 octobre 2016, STMicroelectronics.</i>	[CER]
[ST]	<p>Cible de sécurité de référence :</p> <ul style="list-style-type: none"> <li>- <i>Trusted Platform modules ST33TPHF2X TPM FIRMWARE 1.256, 1.257, 1.258 &amp; 2.256, 2.272 and ST33GTPMA/I TPM firmware 3.256, 3.257 &amp; 6.256, 6.257 - Security Target, reference SSS_ST33TPHF2X_GTPMA_ST_18_001, révision 01.03, daté du 30 juin 2020, STMICROELECTRONICS.</i></li> </ul> <p>Version publique :</p> <ul style="list-style-type: none"> <li>- <i>Trusted Platform modules ST33TPHF2X TPM FIRMWARE 1.256, 1.257, 1.258 &amp; 2.256, 2.272 and ST33GTPMA/I TPM firmware 3.256, 3.257 &amp; 6.256, 6.257 - Security Target, reference SSS_ST33TPHF2X_GTPMA_ST_18_001 public, révision 01.03p, daté du 30 juin 2020, STMICROELECTRONICS.</i></li> </ul>	[R-M03]
[CONF]	<i>TPM FIRMWARE F2X 00.01.01.00 –CONFIGURATION LIST, référence SSS_ST33TPHF2X_HC4_CFGL_19_001, version 1, daté du 21 juin 2019, STMICROELECTRONICS.</i>	[CER]
	<i>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.</i>	[CER]
	<i>TPM FIRMWARE F2X HD8 00.01.01.02 –CONFIGURATION LIST, référence SSS_ST33TPHF2X_HD8_CFGL_20_001, version 1, daté du 19 mars 2020, STMICROELECTRONIC</i>	[R-M02]
	<i>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</i>	[CER]
	<i>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.</i>	[R-M02]
	<i>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.</i>	[CER]
	<i>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.</i>	[CER]
	<i>TPM FIRMWARE F2X ZE4 00.03.01.01 –CONFIGURATION LIST, référence SSS_ST33GTPMISPI_CFGL_20_001, version 1, daté du 4 septembre 2020, STMICROELECTRONICS</i>	[R-M03]
	<i>TPM FIRMWARE F2X ZE5 00.06.01.01 –CONFIGURATION LIST, référence SSS_ST33GTPMII2C_CFGL_20_001, version 1, daté du 4 septembre 2020, STMICROELECTRONICS</i>	[R-M03]

## 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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.eu](http://www.sogis.eu).

<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org).