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-2016/78-M01

ST33TPHF2ESPI mode TPM 2.0 TPM Firmware version 73.04 (0x49.0x04)

Certificat de référence : ANSSI-CC-2016/78

Paris, le 28/06/17

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2016/78, ST33TPHF2ESPI mode TPM 2.0 TPM Firmware version 73.00 (0x49 0x00), 13 décembre 2016, ANSSI.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	ST33TPHF20/ESPI Security Impact Analysis Report between 49/4A.00 and 49/4A.04, reference SSS_ST33TPHF20ESPI_49A04_SIA_17_001, version 01.00, 31 mars 2017, *STMICROELECTRONICS.*
[RM-Lab]	Evaluation Technical Report MOURVEDREV2 M01, référence GREv2M01_ETR, version 2.0, 16 juin 2017, *THALES*.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

2. Identification du produit maintenu

Le composant « ST33TPHF2ESPI mode TPM 2.0, hardware ST33HTPH révision A en externe et C en interne, TPM[1] *firmware* version 73.00[2] », a été initialement certifié sous la référence ANSSI-CC-2016/78 (référence [CER]).

Le produit objet de la présente maintenance est « ST33TPHF2ESPI mode TPM 2.0, hardware ST33HTPH révision A en externe et C en interne, TPM *firmware* version 73.04[3]» développé par la société *STMICROELECTRONICS*.

Les versions maintenues des produits sont identifiables par les éléments suivants :

1) TPM *firmware* en mode TPM 2.0, version 73.00 mis à jour sur le terrain en version 73.04
   - dénomination commerciale du composant ST33TPHF2ESPI pour cette version de *firmware* :
     - soit « P68HAAF1 » (produit en mode TPM 2.0 par défaut) ;
     - ou « P68HAAF0 » (produit en mode TPM 1.2 par défaut configuré en mode TPM 2.0) ;
   - informations inscrites sur la surface du composant :
     - *maskset reference* : K8K0 ;
     - *OST[4] revision (autotest ROM code) : OST 2.2 (*YQBF*)* ;
   - contenu de « TMP_CAP_VENDOR_PROPERTY » obtenu à partir de la commande « TMP_GetCapability » :

[1] *Trusted Platform Module.*
[2] 49.00 en hexadecimal.
[3] 49.04 en hexadecimal.
[4] *Operating System for Test*.

- *hardware Chameleon code :* 41 46 31 00 (AF1) ou 41 46 30 00 (AF0 configuré en TPM 1.2) ;
- *digest factory* (32 bytes) : 30 A2 14 ED F6 3A 25 DB 9A 9B BC AC F1 45 DC E4 A2 7A DF EA 64 CA 79 1A 11 57 B6 F1 A8 A4 3D 50 ;
- *digest current* (32 bytes) : B9 71 31 A2 CF 43 EF C2 8C 8F 7A 4D BC 1E 04 6A B2 96 87 9E 77 A5 8E 2E 7E A4 06 66 E6 70 8D C5 ;

- contenu de « TMP_CAP_TPM_PROPERTIES» obtenu à partir de la commande « TMP_GetCapability » :
  - *TMP firmware version :* 00 49 00 04 ;
  - *internal firmware version :* 44 A0 11 64.

2) TPM *firmware* en mode TPM 2.0, version 73.04 dès la sortie d'usine :
   - dénomination commerciale du composant ST33TPHF2ESPI pour cette version de *firmware* :
     - soit « P68HAHB4 » (produit en mode TPM 2.0 par défaut) ;
     - ou « P68HAHB3 » (produit en mode TPM 1.2 par défaut configuré en mode TPM 2.0) ;
   - informations inscrites sur la surface du composant :
     - *maskset reference* : K8K0 ;
     - *OST[1] revision (autotest ROM code) : OST 2.2 (*YQBF*)* ;
   - contenu de « TMP_CAP_VENDOR_PROPERTY » obtenu à partir de la commande « TMP_GetCapability » :
     - *hardware Chameleon code :* 48 42 34 00 (HB4) ou 48 42 33 00 (HB3 configuré en TPM 2.0) ;
     - *digest factory* (32 bytes) : B9 71 31 A2 CF 43 EF C2 8C 8F 7A 4D BC 1E 04 6A B2 96 87 9E 77 A5 8E 2E 7E A4 06 66 E6 70 8D C5 ;
     - *digest current* (32 bytes) : B9 71 31 A2 CF 43 EF C2 8C 8F 7A 4D BC 1E 04 6A B2 96 87 9E 77 A5 8E 2E 7E A4 06 66 E6 70 8D C5 ;
   - contenu de « TMP_CAP_TPM_PROPERTIES» obtenu à partir de la commande « TMP_GetCapability » :
     - *TMP firmware version :* 00 49 00 04 ;
     - *internal firmware version :* 44 A0 11 64.

3. Description des évolutions

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

- l'ajout d'une résistance de *pull-up* sur la broche « chip select » ;
- la modification de la phase de réveil lorsque le TPM est en mode « basse consommation » ;
- des corrections concernant des erreurs fonctionnelles mineures ;
- des améliorations pour accroître la robustesse du produit ;
- des corrections concernant la mise en conformité avec l'errata 1.5 des spécifications de librairie « TPM 2.0 level 0 revision 1.16 ».

[1] *Operating System for Test*.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) attestant que les évolutions du produit sont bien mineures.

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]	Datasheet - Flash based device combining TPM 1.2 and TPM 2.0 with and SPI interface, référence DS_ST33TPHF2ESPI, version 12, avril 2017, *STMICROELECTRONICS*.	**[R-M01]**
	ST33TPMF2E – Security Guidelines for TPM Configuration, référence SSS_ST33TPMF2E_AN_15_005, version 01.03, 18 décembre 2015, *STMICROELECTRONICS*.	[CER]
	ST33TPHF2ESPI FW 49.04 AGD deliveries, référence SSS_ST33TPHF2ESPI_4904_AGD_17_001, version 01.00, 26 mai 2017, *STMICROELECTRONICS*.	**[R-M01]**
	STSW-TPMCERT1 – ST Trusted Platform Module Endorsement Key certificates, référence DocID028078, version 3 de septembre 2016, *STMICROELECTRONICS*.	[CER]
	ST33TPHF20SPI Security recommendations, référence SSS_TPHF20_AN_16_001, version 01.02 du 27 octobre 2016, *STMICROELECTRONICS*.	[CER]
[ST]	Cible de sécurité de référence : - Trusted Platform Module ST33TPHF2ESPI Mode TPM 2.0 TPM firmware 0X49.0x04, référence SSS_ST33TPHF2ESPI_M20_ST_16_002, version 02.00, 26 mai 2017, *STMICROELECTRONICS*. Version publique : - Trusted Platform Module ST33TPHF2ESPI Mode TPM 2.0 TPM firmware 0X49.0x04, référence SSS_ST33TPHF2ESPI_M20_STP_16_002, version 02.00p, 26 mai 2017, *STMICROELECTRONICS*.	**[R-M01]** **[R-M01]**
[CONF]	Liste de configuration du produit : - TPM Firmware F2E 0x49 0x04 for chip « HB3 & HB4 » configuration list, référence SSS_TPMF2E_4904_HB34_CFGL_17_001, version 01.00, 26 mai 2017, S*TMICROELECTRONICS*. - ST33HTPH rev C & ST_Firmware rev1 (ext) rev1 (int) configuration list, référence SMD_33HTPM_HTPH_CFGL_16_001, version 01.01, *STMICROELECTRONICS*.	**[R_M01]** [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. 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 la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. 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 CC RA [CC RA].

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] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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