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-2016/43-M01

ST33TPHF2ESPI mode TPM 2.0
TPM Firmware version 71.12 (0x47 0x0C)

Certificat de référence : ANSSI-CC-2016/43

Paris, le 16 février 2017

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-2016/43, ST33TPHF2ESPI mode TPM 2.0 TPM Firmware version 47.00 et version 47.04 du 4 juillet 2016.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	ST33TPHF2ESPI Security Impact Analysis between 47.04 and 47.0C, référence SSS_ST33TPHF2ESPI_SIA_17_001, version 01.01 du 24 janvier 2017, *STMICROELECTRONICS.*
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 8th, 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.

2. Identification du produit maintenu

Le produit « ST33TPHF2ESPI mode TPM 2.0, hardware ST33HTPH révision A en externe et C en interne, TPM *firmware* version 47.00 et version 47.04 » a été initialement certifié sous la référence ANSSI-CC-2016/43 (référence [CER]).

Le produit objet de la présente maintenance, est le composant « ST33TPHF2ESPI mode TPM 2.0, hardware ST33HTPH révision A en externe et C en interne, TPM *firmware* version 47.0C[1]» développé par *STMICROELECTRONICS.*

La version maintenue du produit est identifiable par les éléments suivants :

- TPM *firmware* version 47.00 pré-chargé en mode TPM 2.0 mis à jour sur le terrain en version 47.0C :
  - marquage externe P68HAAE6 qui est la dénomination commerciale du composant ST33TPHF2ESPI pour cette version de *firmware* ;
  - informations inscrites sur la surface du composant :
    - *maskset reference* : K8K0 ;
    - *OST revision* (autotest ROM code) : OST 2.2 (YQBF).
  - contenu de « TMP_CAP_VENDOR_PROPERTY » obtenu à partir de la commande « TMP2_GetCapability » :
    - *hardware Chameleon code : 41 45 36 00 (AE6) ;*
  - *digest factory* (32 *bytes*) *:* 98 CE 78 4D FA 26 2A 9F 2F C7 8C 6A 17 21 18 5F 5C CA 30 59 5D 2D B2 47 7B 75 8D 4D 37 0B 49 1D ;
  - *digest current* (32 *bytes*) *:* 7F C6 EA 6C D7 9F 5D A7 4D 24 DC 22 2A F2 41 71 70 9D EA E5 21 FA D9 02 36 2D 09 C0 67 AB 64 08 ;
  - contenu de « TMP_CAP_TPM_PROPERTIES» obtenu à partir de la commande « TMP_GetCapability » :
    - TMP *firmware version* : **00 47 00 0C** ;
    - *internal firmware version* : **44 A0 10 04**.

[1] Version exprimée en hexadécimal.

- TPM *firmware* version 47.04 pré-chargée en mode TMP 2.0 mis à jour sur le terrain en version 47.0C :
  - marquage externe P68HAHA6 qui est la dénomination commerciale du composant ST33TPHF2ESPI pour cette version de *firmware* ;
  - informations inscrites sur la surface du composant :
    - *maskset reference* : K8K0 ;
    - *OST revision* (autotest ROM code) : OST 2.2 (YQBF) ;
  - contenu de « TMP_CAP_VENDOR_PROPERTY » obtenu à partir de la commande « TMP2_GetCapability » :
    - *hardware Chameleon code* : 48 41 36 00 (HA6) ;
  - *digest factory* (32 *bytes*) *:* BD AD 44 28 69 F3 E4 38 2E 84 C6 60 C9 4D 27 8C 90 23 81 CC D0 40 BE D2 DB 1C 6A ED 27 91 45 CD ;
  - *digest current* (32 *bytes*) *:* 7F C6 EA 6C D7 9F 5D A7 4D 24 DC 22 2A F2 41 71 70 9D EA E5 21 FA D9 02 36 2D 09 C0 67 AB 64 08 ;
  - la version logicielle est obtenue à partir de la commande « TMP_GetCapability » qui pour les *tags* TPM_PT_FIRMWARE_VERSION_1 et TPM_PT_FIRMWARE_VERSION_2 renvoie respectivement les données :
    - TMP *firmware version* : **00 47 00 0C** ;
    - *internal firmware version* : **44 A0 10 04**.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que douze modifications n'affectant pas la sécurité du produit ont été opérées. Ces modifications concernent :

- les objets persistants ayant comme attribut « NoDa » qui sont maintenant utilisables même si le mécanisme contre l'attaque par dictionnaire est activé ;
- le réveil lorsque le TPM est en mode basse consommation ;
- le traitement du paramètre « authValue » lorsqu'il contient des valeurs nulles lors du traitement des commandes TPM2_HMAC_Start et TPM2_HashSequenceStart ;
- le code retourné lors de la création d'une session d'autorisation lorsque la clé de chiffrement n'est pas une clé asymétrique ;
- le calcul de l'incrément du vecteur IV pour le chiffrement en mode CRT ;
- la remise à leur valeur initiale de certains *flags* lors du traitement de la commande TPM2_HierarchyChangeAuth ;
- certaines sections non sauvegardées qui sont maintenant systématiquement purgées après le redémarrage du TPM ;
- le code de retour suite à une commande TPM2_Create ;
- le code d'erreur retourné qui était parfois erroné suite à une commande longue utilisant une session de chiffrement / déchiffrement ;
- l'incrément automatique du compteur « DA » sans que la commande TPM2_Shutdown soit exécutée ;
- le protocole de communication SPI pour supporter des écritures de blocs de plus de quatre bytes à la fois ;
- le traitement du cas d'erreur lors de la création d'objets avec des paramètres non supportés par le TMP.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables, du produit évalué et sont 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 9 de janvier 2017, *STMICROELECTRONICS*.	[R-M01]
	TPM EK certificate chip and EK authenticity verification, référence SSS_TPMEK_UM_15_001, version 02-00 du 11 mars 2016, *STMICROELECTRONICS*.	[CER]
	ST33TPMF2E – Security Guidelines for TPM Configuration, référence SSS_ST33TPMF2E_AN_15_005, version 01-03 du 18 décembre 2015, *STMICROELECTRONICS*.	[CER]
	ST33TPHF2ESPI – AGD deliveries, référence SSS_ST33TPHF2ESPI_AGD_16_001, version 01-01 du 30 janvier 2017, *STMICROELECTRONICS*.	[R-M01]
[ST]	Cibles de sécurité de référence : - ST33TPHF2ESPI_M20_ST, référence SSS_ST33TPHF2ESPI_M20_ST_16_001, version 01.02 du 30 janvier 2017, *STMICROELECTRONICS*. Pour les besoins de publication, la cible de sécurité suivante a été fournie : - ST33TPHF2ESPI_M20_ST, référence SSS_ST33TPHF2ESPI_M20_STP_16_001, version 01.02p du 30 janvier 2017, *STMICROELECTRONICS*.	[R-M01]
[CONF]	TPM firmware F2E 0x47.0x0C configuration list, référence SSS_TPMF2E_470C_CFGL_17_001, version 01-00 du 30 janvier 2017, *STMICROELECTRONICS*.	[R-M01]
	NesLib 4.2.9 for ST33 on ST33HTPH configuration list, référence SSS_NesLib429ST33_HTPH_CFGL_15_001, version 01-00 du 13 octobre 2015, *STMICROELECTRONICS*.	[CER]
	ST33HTPH rev C & ST_Firmware rev1(ext) rev1(int) configuration list, référence SMD_33HTPM_HTPH_CFGL_16_001, version 01.01, *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. 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.