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-2020/24-M01

ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM

Certificat de référence : ANSSI-CC-2020/24

Paris, le 25 novembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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

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

1 Références

[CER]	Rapport de certification ANSSI-CC-2020/24, ST33G1M2A1 C01 including optional cryptographic library NesLib and optional library SFM, 14 mai 2020.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	Security Impact Analysis Report – ST33G1M2A1 C02, version SMD_ST33G1M2A1_C02_SIA_20_001, révision1.0, août 2020.
[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 « ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM » développé par la société STMicroelectronics. ST33G1M2A1 C02 correspond au microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique NesLib 6.3.4 et la bibliothèque SFM 1.0.8. (référence [ST]).

Le produit « ST33G1M2A1 C01 » a été initialement certifié sous la référence ANSSI-CC-2020/24 (référence [CER]).

3 Description des évolutions

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

- mise à jour de la librairie SFM de la version 1.0.7 à la version 1.0.8 pour correction de *bugs* fonctionnels liés à l'activation de la fonctionnalité de répartition de l'usure de la mémoire (« *wear-leveling* ») et à la fonction de défragmentation de la mémoire.

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]	*ST33G Platform–ST33G1M2A:Secure MCU with 32-bit ARM SecurCore SC300 CPU and high density Flash memory – Datasheet*, référence DS_ST33G1M2A, version 3.0 .	[CER]
	ST33G1M2A, ST33G1M2M: CMOS M10+ 80-nm technology die and wafer delivery description, référence DD_ST33G1M2A_M, version 2.0 .	[CER]

	ARM Cortex SC300 r0p0 Technical Reference Manual, référence ARM DDI 0337F, version F .	[CER]
	ARM Cortex M3 r2p0 Technical Reference Manual, référence ARM DDI 0337F3c, version F3c .	[CER]
	ST33G1M2A / ST33G1M2M firmware -User manual, référence UM_ST33G1M2A_M_FW, version 11 .	[CER]
	Flash memory loader installation guide for ST33G1M2A and ST33G1M2M platforms, référence UM_33GA_FL, version 3.0 .	[CER]
	ST33G and ST33H Firmware support for LPU regions – application note, référence AN_33G_33H_LPU, version 1 .	[CER]
	ST33G and ST33H SecureMCU platforms –Securiy Guidance, référence AN_SECU_ST33, version 9 .	[CER]
	ST33G and ST33H Power supply glitch detector characteristics –application note, référence AN_33_GLITCH, version 2 .	[CER]
	ST33G and ST33H –AIS31 Compliant Random Number –User Manual, référence UM_33G_33H_AIS31, version 3 .	[CER]
	ST33G and ST33H –AIS31 –Reference implementation: Start-up, on-line and total failure tests –Application note, référence AN_33G_33H_AIS31, version 1 .	[CER]
	NesLib cryptographic library NesLib 6.3 –User manual, référence UM_NesLib_6.3, version 4 .	[CER]
	ST33G and ST33H secure MCU platforms –NesLib 6.3 security recommendations –Application note, référence AN_SECU_ST33G_H_NESLIB_6.3, version 5 .	[CER]
	NesLib 6.3.4for ST33G, ST33H and ST33I platforms –Release note, référence RN_ST33_NESLIB_6.3.4, version 2 .	[CER]
	ST33 uniform timing application note, référence AN_33_UT, version 2 .	[CER]
	StoreKeeper v1.0 –User manual, référence UM_StoreKeeper, version 3 .	[CER]
	Security recommendation Application Note SFM Library 1.0, référence AN_SECU_StoreKeeper, version1.	[CER]
[ST]	Cibles de sécurité de référence: *ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM, Security Target* ; SMD_ST33G1M2A1_ST_19_001 rev C02 septembre 2020 ; Version publique : . *ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM, Security Target For Composition* ; SMD_ST33G1M2A1_ST_19_002 rev C02 septembre 2020.	[R-M01]
[CONF]	*ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM- Configuration List, SMD_33G_CFGL_16_002, rev 1.04*, septembre 2020.	[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.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

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.

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.eu.

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