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 surveillance ANSSI-CC-2020/24-S02

ST33G1M2A1 C03 including optional cryptographic library NesLib and optional library SFM

Certificat de référence : ANSSI-CC-2020/24

Paris, le 08/09/2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

AVERTISSEMENT

La surveillance du produit ne constitue pas en soi une recommandation d'utilisation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit soit totalement exempt de vulnérabilités exploitables.

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-2020/24, ST33G1M2A1 C01 including optional cryptographic library NesLib and optional library SFM, version C01, 14 mai 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2020/24-S01, ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM, version C02, 7 juillet 2021.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[R-M01]	Rapport de maintenance ANSSI-CC-2020/24-M01, ST33G1M2A1 C02 including optional cryptographic library NesLib and optional library SFM, version C02, 20 novembre 2020.
[R-M02]	Rapport de maintenance ANSSI-CC-2020/24-M02, ST33G1M2A1 C03 including optional cryptographic library NesLib and optional library SFM, version C03.
[RS-Lab]	*Evaluation Technical Report ASTIAM2 2022 / ST33G1M2A1*, référence ASTIM2_2022_ETR, version 1.0, 13 juillet 2022, THALES / CNES.
[ETR_COMP]	Pour le besoin des évaluations ou surveillances en composition avec ce produit le rapport technique pour la composition a été mis à jour : *Evaluation Technical Report ASTIAM2 2022 / ST33G1M2A1*, référence ASTIM2_2022_ETRLite, version 1.0, 13 juillet 2022, THALES / CNES.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation THALES / CNES, permet d'attester que le produit « ST33G1M2A1 C03 including optional cryptographic library NesLib and optional library SFM », initialement certifié sous la référence [CER], peut être considéré comme résistant à des attaques de niveau AVA_VAN.5 dans les mêmes conditions et restrictions d'usage que celles définies dans [CER], complétées par les mises à jour des guides [GUIDES] intégrées au fil de la maintenance [R-M02].

Ce résultat est applicable au produit « ST33G1M2A1 C03 including optional cryptographic library NesLib and optional library SFM » maintenu sous la référence [R-M02].

Le rapport d'évaluation pour composition [ETR_COMP] a été mis à jour pour refléter les résultats de cette dernière surveillance.

Le rapport de surveillance [RS-Lab] permet également d'attester que le cycle de vie du produit est conforme aux composants de la classe ALC définis dans [CER].

La périodicité de la surveillance de ce produit est de 1 an.

3 Guides applicables

Le tableau ci-dessous liste les guides applicables du produit évalué. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du guide correspondant.

Les guides correspondants ne contiennent pas de nouvelle recommandation sécuritaire.

[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, 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 Secure MCU 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 6.	[R-M02]
	NesLib 6.3.4 for ST33G, ST33H and ST33I platforms – Release note, référence RN_ST33_NESLIB_6.3.4, version 3.	[R-M02]
	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, version 1.	[CER]