



**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-2020/25-S02

ST33H768 C02 including optional cryptographic library NesLib and optional technology MIFARE4Mobile

Certificat de référence : ANSSI-CC-2020/25

Paris le 06/09/2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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

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

1 Références

[CER]	Rapport de certification ANSSI-CC-2020/25, ST33H768 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile, version C01, 14 mai 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2020/25-S01, ST33H768 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile, version C01, 7 juillet 2021.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[R-M01]	Rapport de maintenance ANSSI-CC-2020/25-M01, ST33H768 C02 including optional cryptographic library NesLib and optional technology MIFARE4Mobile, version C02.
[RS-Lab]	<i>Evaluation Technical Report ASTI2M Maint 2022 / ST33H768 C02</i> , référence ASTI2M_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 : <i>Evaluation Technical Report ASTI2M Maint 2022 / ST33H768 C02</i> , référence ASTI2M_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 « ST33H768 C02 including optional cryptographic library NesLib and optional technology MIFARE4Mobile », 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-M01].

Ce résultat est applicable au produit « ST33H768 C02 including optional cryptographic library NesLib and optional technology MIFARE4Mobile » maintenu sous la référence [R-M01].

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]	<i>ST33H768 Secure MCU with 32-bit ARM SecurCore SC300 – Datasheet</i> , référence DS_ST33H768, version 4.	[CER]
	<i>ST33H768 platform : BP and BM specific product profiles – Technical note</i> , référence TN_ST33H768_01, version 1.0.	[CER]
	<i>ST33 H768 platform : LS, LC and BS specific product profiles – Technical note</i> , référence TN_ST33 H768_02, version 1.0.	[CER]
	<i>ST33 H768 : CMOS M10+ 80-nm technology die and wafer delivery description</i> , référence DD_ST33 H768, version 2.0.	[CER]
	<i>ARM Cortex SC300 r0p0 Technical Reference Manual</i> , référence ARM DDI 0337F, version F.	[CER]
	<i>ARM Cortex M3 r2p0 Technical Reference Manual</i> , référence ARM DDI 0337F3c, version F3c.	[CER]
	<i>ST33 H768 Firmware user manual</i> , référence UM_ST33 H768_FW, version 10.	[CER]
	<i>ST33 H768 and derivatives Flash loader installation guide</i> , référence UM_33H_FL, version 4.0.	[CER]
	<i>ST33G and ST33H Firmware support for LPU regions – application note</i> , référence AN_33G_33H_LPU, version 1.	[CER]
	<i>ST33G and ST33H Secure MCU platforms – Security Guidance</i> , référence AN_SECU_ST33, version 9.	[CER]
	<i>ST33G and ST33H Power supply glitch detector characteristics – application note</i> , référence AN_33_GLITCH, version 2.	[CER]
	<i>ST33G and ST33H – AIS31 Compliant Random Number – User Manual</i> , référence UM_33G_33H_AIS31, version 3.	[CER]
	<i>ST33G and ST33H – AIS31 – Reference implementation : Start-up, on-line and total failure tests – Application note</i> , référence AN_33G_33H_AIS31, version 1.	[CER]
	<i>ST33 uniform timing application note</i> , référence AN_33_UT, version 2.	[CER]
	<i>NesLib cryptographic library NesLib 6.3 – User manual</i> , référence UM_NesLib_6.3, version 4.	[CER]
	<i>ST33G and ST33H secure MCU platforms – NesLib 6.3 security recommendations – Application note</i> , référence AN_SECU_ST33G_H_NESLIB_6.3, version 6.	[R-M01]
	<i>NesLib 6.3.4 for ST33G, ST33H and ST33I platforms – Release note</i> , référence RN_ST33_NESLIB_6.3.4, version 3.	[R-M01]
	<i>MIFARE4Mobile library 2.1 – User manual</i> , référence UM_33_MIFARE4Mobile-2.1, version 5.	[CER]
	<i>MIFARE4Mobile library 2.1.0 for ST33G1M2 – Application note</i> , référence AN_ST33G1M2_M4M_Lib, version 1.	[CER]