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-2020/25-M01

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

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

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.
[R-S02]	Rapport de surveillance ANSSI-CC-2020/25-S02, ST33H768 C02 including optional cryptographic library NesLib and optional technology MIFARE4Mobile, version C02.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	*Security impact analysis report - ST33GH C02 C03 D01*, référence SMD_ST33GH_C02_C03_D01_SIA_22_001, version 1.1.
[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 « ST33H768 C02 including optional cryptographic library NesLib and optional technology MIFARE4Mobile[Catégorie] » développé par la société STMICROELECTRONICS.

Le produit « ST33H768 C01 » a été initialement certifié sous la référence ANSSI-CC-2020/25 (référence [CER]).

Il a déjà fait l'objet de surveillances sous les références ANSSI-CC-2020/25-S01 (référence [R-S01]) et ANSSI-CC-2020/25-S02 (référence [R-S02]).

3 Description des évolutions

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

- Clarification de la taille minimale des clés RSA dans la cible de sécurité ;
- Clarification d'une mention concernant le DES dans la cible de sécurité ;
- Référencemement de guides provenant d'organismes de certification ou de standardisation concernant l'utilisation de mécanismes cryptographiques dans une note d'application.

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]	*ST33H768 Secure MCU with 32-bit ARM SecurCore SC300 – Datasheet*, référence DS_ST33H768, version 4.	[CER]
	ST33H768 platform : BP and BM specific product profiles – Technical note, référence TN_ST33H768_01, version 1.0.	[CER]
	ST33 H768 platform : LS, LC and BS specific product profiles – Technical note, référence TN_ST33 H768_02, version 1.0.	[CER]
	ST33 H768 : CMOS M10+ 80-nm technology die and wafer delivery description, référence DD_ST33 H768, 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]
	ST33 H768 Firmware user manual, référence UM_ST33 H768_FW, version 10.	[CER]
	ST33 H768 and derivatives Flash loader installation guide, référence UM_33H_FL, version 4.0 .	[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]
	ST33 uniform timing application note, référence AN_33_UT, version 2.	[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-M01]
	NesLib 6.3.4 for ST33G, ST33H and ST33I platforms – Release note, référence RN_ST33_NESLIB_6.3.4, version 3.	[R-M01]
	MIFARE4Mobile library 2.1 – User manual, référence UM_33_MIFARE4Mobile-2.1, version 5.	[CER]
	MIFARE4Mobile library 2.1.0 for ST33G1M2 – Application note, référence AN_ST33G1M2_M4M_Lib, version 1.	[CER]

[ST]	Cibles de sécurité de référence : *ST33H768 C02 including optional cryptographic library NesLib, and optional technology MIFARE4Mobile® Security Target*, référence SMD_ST33H768_ST_19_001, version C02.0, 26 avril 2022. Version publique : *ST33H768 C02 including optional cryptographic library NesLib, and optional technology MIFARE4Mobile® Security Target for composition*, référence SMD_ST33H768_ST_19_002, version C02.0, avril 2022	[R-M01]
[CONF]	*ST33H768 C02 Configuration List*, référence SMD_K8K0_C_CFGL_22_001, version 1.	[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.