PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

**Secrétariat général de la défense
et de la sécurité nationale**

Rapport de maintenance
ANSSI-CC-2019/40-M02

ST31H320

D05

Certificat de référence : ANSSI-CC-2019/40

Paris le 15 septembre 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-2019/40, ST31H320 D01, 29 novembre 2019
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01
[R-S01]	Rapport de surveillance ANSSI-CC-2019/40-S01, ST31H320 D02, 29 septembre 2020
[R-S02]	Rapport de surveillance ANSSI-CC-2019/40-S02, ST31H320 D03, 23 septembre 2021
[R-S03]	Rapport de surveillance ANSSI-CC-2019/40-S03, ST31H320 D05
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01
[R-M01]	Rapport de maintenance ANSSI-CC-2019/40-M01, ST31H320 D03, 23 septembre 2021
[IAR]	Security impact analysis report, ST31H320 D04, ST31H320_D04_SIA, mai 2022
[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 « ST31H320 D05 » développé par la société STMICROELECTRONICS ; il a été initialement certifié sous la référence ANSSI-CC-2019/40 (référence [CER]).

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne une clarification de la taille minimale des clés RSA dans la cible de sécurité.

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-M02] référence la présente maintenance.

[GUIDES]	*ST31H platform ST31H320, Datasheet – production data, DS_ST31H320 Rev 2*, 29 janvier 2016, STMicroelectronics	[CER]
	ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, septembre 2010, ARM	[CER]
	ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, septembre 2010, ARM	[CER]
	User manual, ST31 firmware, UM_ST31G_H_FWv3 Rev 9, mars 2019, STMicroelectronics	[CER]
	User manual, NesLib cryptographic library NesLib 6.2, UM_NesLib_6.2 Rev 3, mars 2020, STMicroelectronics	[R-S01]
	Application note, ST31G and ST31H secure MCU platforms NesLib 6.2 security recommendations, AN_SECU_ST31G_H_NESLIB_6.2 Rev9, juin 2022, STMicroelectronics	[R-S03]
	Release note, NesLib 6.2.1 for ST31G and ST31H platforms, RN_ST31_NESLIB_6.2.1 – Rev 7, juillet 2022, STMicroelectronics	[R-S03]
	ST31H and ST31H Secure MCU platforms Security Guidance, AN_SECU_ST31G_H, version 10, avril 2021, STMicroelectronics	[R-S02]
	User manual, ST31G and ST31H – AIS31 Compliant Random Number, UM_31G_31H_AIS31 Rev1, janvier 2015, STMicroelectronics	[CER]
	Application note, ST31G and ST31H – AIS31 reference implementation: start-up, on-line and total failure tests, AN_31G_31H_AIS31 Rev 1, janvier 2015, STMicroelectronics	[CER]
[ST]	*ST31H320 D05 including optional cryptographic library NESLIB, Security Target for composition, SMD_ST31H320_ST_19_002 rev D05.1*, juillet 2022	[R-M02]
[CONF]	*ST31H320_TOE_Refs_D05_1*, juillet 2022	[R-M02]

5 Conclusions

Les évolutions décrites ci-dessus sont considérées comme ayant un impact mineur.

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 :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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.

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