



**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-2019/40-M01

ST31H320

D03

Certificat de référence : ANSSI-CC-2019/40

Paris le 23 septembre 2021

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

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

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
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01
[IAR]	Security impact analysis report, ST31H320 D03, ST31H320_D03_SIA, avril 2021
[RM-Lab]	Surveillance Technical Report – Loupiac3 & Loupiac4 projet, Loupiac3_C03_Loupiac4_D03_STR_v1.0, 26 juillet 2021, SERMA SAFETY & SECURITY
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee</i>
[CCRA]	<i>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014</i>

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « ST31H320 D03 » 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 que le cycle de vie du produit a été modifié : certains sites sont utilisés pour moins d'activités, l'adresse de certains sites est modifiée.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

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]	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 Rev8, septembre 2019, STMicroelectronics	[CER]
	Release note, NesLib 6.2.1 for ST31G and ST31H platforms, RN_ST31_NESLIB_6.2.1 – Rev 6, mars 2020, STMicroelectronics	[R-S01]
	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 D03 including optional cryptographic library NESLIB, Security Target for composition, SMD_ST31H320_ST_19_002 rev D03.0, juin 2021	[R-M01]
[CONF]	ST31-K8N0-Configuration List –D03, ST31H320_J_CFGL_D03 rev1.0, avril 2021	[R-M01]

5 Conclusions

Les évolutions décrites ci-dessus, relatives au cycle de vie, 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'accord¹, 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 signataires², 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.