



**PREMIÈRE  
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-2019/40-S03

## 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

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](mailto: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-S01, ST31H320 D03, 23 septembre 2021
[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
[R-M02]	Rapport de maintenance ANSSI-CC-2019/40-M02, ST31H320 D05
[RS-Lab]	<i>Surveillance Technical Report – Loupiac3 &amp; Loupiac4 projet, Loupiac3_C05_Loupiac4_D05_STR_v1.0</i> , 19 août 2022, SERMA SAFETY & SECURITY.
[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>Surveillance Technical Report Lite for Composition – Loupiac4 projet, Loupiac4_D05_STR_Lite_v1.0</i> , 19 août 2022, SERMA SAFETY & SECURITY.

## 2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation SERMA SAFETY & SECURITY, permet d'attester que le produit « ST31H320 D05 », 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 recommandations sécuritaires additionnelles intégrées au fil des surveillances successives dans [GUIDES].

Il est à noter que de nouvelles recommandations sécuritaires ont été ajoutées au titre de la présente surveillance. Si ces recommandations ne sont pas mises en œuvre, le produit ne peut pas être considéré comme résistant à des attaques de niveau AVA\_VAN.5.

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 décrits dans la cible de sécurité (voir [R-M02]).

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.

En particulier, [R-S03] référence la présente surveillance.

Les guides contenant de nouvelles recommandations sécuritaires par rapport à la précédente surveillance apparaissent en gras.

[GUIDES]	<i>ST31H platform ST31H320, Datasheet – production data, DS_ST31H320 Rev 2, 29 janvier 2016, STMicroelectronics</i>	[CER]
	<i>ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, septembre 2010, ARM</i>	[CER]
	<i>ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, septembre 2010, ARM</i>	[CER]
	<i>User manual, ST31 firmware, UM_ST31G_H_FWv3 Rev 9, mars 2019, STMicroelectronics</i>	[CER]
	<i>User manual, NesLib cryptographic library NesLib 6.2, UM_NesLib_6.2 Rev 3, mars 2020, STMicroelectronics</i>	[R-S01]
	<b>Application note, ST31G and ST31H secure MCU platforms NesLib 6.2 security recommendations, AN_SECU_ST31G_H_NESLIB_6.2 Rev9, juin 2022, STMicroelectronics</b>	[R-S03]
	<i>Release note, NesLib 6.2.1 for ST31G and ST31H platforms, RN_ST31_NESLIB_6.2.1 – Rev 7, juillet 2022, STMicroelectronics</i>	[R-S03]
	<i>ST31H and ST31H Secure MCU platforms Security Guidance, AN_SECU_ST31G_H, version 10, avril 2021, STMicroelectronics</i>	[R-S02]
	<i>User manual, ST31G and ST31H – AIS31 Compliant Random Number, UM_31G_31H_AIS31 Rev1, janvier 2015, STMicroelectronics</i>	[CER]
	<i>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</i>	[CER]