



**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-2020/04-S02**

**ST31P450 A03**

**Certificat de référence : ANSSI-CC-2020/04**

Paris, le 2 février 2022

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

Emmanuel NAEGELEN

[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-2020/04, ST31P450 A02, 18 février 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2020/04-S01 ST31P450 A02, 4 novembre 2020.
[RS-Lab]	<i>Evaluation Technical Report, Project MANDALA A03 Surveillance</i> , référence MANDALA_A03_Surv2021_ETR, version 2.0, émis par le CESTI THALES / CNES le 13 janvier 2022.
[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 for composite evaluation, Project MANDALA A03 Surveillance</i> , référence MANDALA_A03_Surv2021_ETRLite, version 2.0, émis par le CESTI THALES / CNES le 13 janvier 2022.

## 2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation THALES / CNES, permet d'attester que le produit « ST31P450 A03 », 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], lorsque les guides applicables [GUIDES] sont respectés.

Le rapport d'évaluation pour composition [ETR\_COMP] a été mis à jour pour refléter les résultats de cette dernière surveillance.

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.

[GUIDES]	<i>Secure dual interface MCU with enhanced security and up to 450 Kbytes of Flash memory- ST31P450 datasheet, référence DS_ST31P450, version 2.0</i>	[CER]
	<i>ARM® Cortex SC000 Technical Reference Manual, référence ARM DDI 0456, version A</i>	[CER]
	<i>ARMv6-M Architecture Reference Manual, référence ARM DDI 0419, version C</i>	[CER]
	<i>ST31P450 Firmware V3 - User Manual, référence UM_ST31P450_FWv3, version 6.0</i>	[CER]
	<i>ST31P secure MCU platform Security guidance – Application Note, référence AN_SECU_ST31P, version 2.0</i>	[R-S01]
	<i>ST31P platform random number generation - User manual, référence UM_ST31P_TRNG, version 2.0</i>	[CER]
	<i>ST31P platform TRNG reference implementation: compliance tests, référence AN_ST31P_TRNG, version 1.0</i>	[CER]