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-2020/05-S01

ST31P450 B02 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1

Certificat de référence : ANSSI-CC-2020/05

Paris, le 4 novembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

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

1 Références

[CER]	Rapport de certification ANSSI-CC-2020/05, ST31P450 B02 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1, 18 février 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[RS-Lab]	Evaluation Technical Report, Project MANDALA with library Surveillance, référence MANDALA_B03_Surv2020_ETR, version 1.0 émis par le CESTI THALES le 15 septembre 2020.
[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 : Evaluation Technical Report for composite evaluation, Project MANDALA with library Surveillance, référence MANDALA_B03_Surv2020_ETRLite, version 1.0 émis par THALES le 15 septembre 2020.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation THALES, permet d'attester que le produit « ST31P450 B03 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1 », 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, 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 être considéré comme résistant qu'à des attaques de niveau AVA_VAN.4.

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.

En particulier, [R-S01] référence la présente surveillance.

Les guides contenant de nouvelles recommandations sécuritaires par rapport au certificat initial apparaissent en gras.

[GUIDES]	Secure dual interface MCU with enhanced security and up to 450 Kbytes of Flash memory- ST31P450 datasheet, référence DS_ST31P450, version 2.0.	[CER]
	ARM® Cortex SC000 Technical Reference Manual, référence ARM DDI 0456, version A.	[CER]
	ARMv6-M Architecture Reference Manual, référence ARM DDI 0419, version C.	[CER]
	ST31P450 Firmware V3 - User Manual, référence UM_ST31P450_FWv3, version 6.0.	[CER]
	ST31P secure MCU platform Security guidance – Application Note, référence AN_SECU_ST31P, version 2.0.	[R-S01]
	ST31P platform random number generation - User manual, référence UM_ST31P_TRNG, version 2.0.	[CER]
	ST31P platform TRNG reference implementation: compliance tests, référence AN_ST31P_TRNG, version 1.0.	[CER]
	Cryptographic library NesLib 6.4 - User manual, référence UM_NesLib_6.4, version 3.0.	[CER]
	ST31P secure MCU platforms NesLib 6.4 security recommendations - Application note, référence AN_SECU_ST31P_NESLIB_6.4, version 5.0.	**[R-S01]**
	NesLib 6.4 for ST31 Platforms - Release note, référence RN_ST31P_NESLIB_6.4.7, version 4.0.	**[R-S01]**
	MIFARE Plus EV1 library v1.1 for the ST31P platform devices - User manual, référence UM_ST31P_MFP_EV1, version 4.0.	**[R-S01]**
	MIFARE Plus EV1 library 1.1.2 on ST31P450 : Release Note, référence RN_ST31P_MFP_EV1_1.1.2, version 2.0.	**[R-S01]**
	MIFARE Plus X and MIFARE PLUS EV1 IV manipulation attack and mitigations, reference TN_MFP_IV, version 1.0.	**[R-S01]**