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-2020/05-M01

ST31P450 B04 including optional cryptographic library NESLIB version 6.4.7 and optional technology MIFARE Plus® EV1 version 1.1.2

Certificat de référence : ANSSI-CC-2020/05

Fait le 2 février 2022

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2020/05, ST31P450 B02, 18 février 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2020/05-S01 ST31P450 B02 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1, 4 novembre 2020.
[R-S02]	Rapport de surveillance ANSSI-CC-2020/05-S02 ST31P450 B03 including optional cryptographic library NESLIB version 6.4.7 and optional technology MIFARE Plus® EV1 version 1.1.2.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01
[IAR]	*SECURITY IMPACT ANALYSIS REPORT – ST31P450 B04 including optional cryptographic library Neslib and optional technology MIFARE Plus® EV1*, référence ST31P450_B04_SIA_21_001, version 1.0, 11 août 2021.
[RM-Lab]	*Evaluation Technical Report, Project MANDALA with library Surveillance*, référence MANDALA_B03_Surv2021_ETR, version 2.0 émis par le CESTI THALES / CNES le 13 janvier 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 le microcontrôleur « ST31P450 B04 including optional cryptographic library NESLIB version 6.4.7 and optional technology MIFARE Plus® EV1 version 1.1.2 » développé par la société STMICROELECTRONICS.

Ce produit a été initialement certifié sous la référence ANSSI-CC-2020/05 (référence [CER]).

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- mise à jour de sites : modification des activités associées à certains sites, suppression d'un site ;
- mise à jour de documents (voir chapitre suivant).

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]	*Secure dual interface MCU with enhanced security and up to 450 Kbytes of Flash memory- ST31P450 datasheet*, référence DS_ST31P450, version 3.0	[R-M01]
	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 7.0	[R-M01]
	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, référence TN_MFP_IV, version 1.0.	[R-S01]
[ST]	Cibles de sécurité de référence : *ST31P450 B04 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1 Security Target*, référence SMD_ST31P450_ST_19_001, version B04.1, 31 août 2021 ; Version publique : *ST31P450 B04 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1 Security Target for composition*, référence SMD_ST31P450_ST_19_002, version B04.1, 31 août 2021.	[R-M01]
[CONF]	*ST31P450 B04 – CONFIGURATION LIST*, référence SMD_ST31P450_CFGL_B04, version 1.0	[R-M01]

5 Conclusions

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

Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

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 :

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.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. 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.

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