PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de surveillance ANSSI-CC-2014/95-S04

Microcontrôleur sécurisé ST31-K330A révision I pour version contact seulement, incluant optionnellement la librairie cryptographique Neslib révision 3.2

Certificat de référence : ANSSI-CC-2014/95

Paris, le 5 octobre 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Microcontrôleur sécurisé ST31-K330A révision I pour version contact seulement, incluant optionnellement la librairie cryptographique Neslib v3.2, 5 janvier 2015, ANSSI-CC-2014/95.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2014/95-S01, 21 août 2015, ANSSI.
[R-S02]	Rapport de surveillance ANSSI-CC-2014/95-S02, 7 septembre 2016, ANSSI.
[R-S03]	Rapport de surveillance ANSSI-CC-2014/95-S03, 18 janvier 2018, ANSSI.
[RS-Lab]	S04 - Surveillance Technical Report - CHABLIS-2 Project, référence CHABLIS-2_STR_v4.0, version 4.0, 14 juin 2018, *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 : S04-Surveillance Technical Lite Report (report for composition) - CHABLIS-2 Project, référence CHABLIS-2_STR-Lite_v4.0, version 4.0, 14 juin 2018, *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 « Microcontrôleur sécurisé ST31-K330A révision I pour version contact seulement incluant optionnellement la librairie cryptographique Neslib v3.2 », 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]	*ST31 – K330 platform (Sx31Zxxx, Mx31Zxxx) – Datasheet*, référence DS_ST31-K330A, version 7, août 2016, *ST MICROELECTRONICS*.	[R-S03]
	ST31 - K330 Platform - Die description, mars 2015, référence DD_31Z052, révision 5, *ST MICROELECTRONICS*.	[R-S03]
	Application note – ST31-K330 security guidance, référence AN_SECU_ST31-K330, version 4, 5 septembre 2014, *ST MICROELECTRONICS*.	[CER]
	Application note – ST31-K330 Dual interface secure microcontrollers - Recommendations for contactless operations, référence AN_31_RCMD, version 2, 28 juillet 2014, *ST MICROELECTRONICS*.	[CER]
	ST31 NesLib cryptographic library - User manual, référence UM_31_NESLIB_3.2, version 7, 24 avril 2014, *ST MICROELECTRONICS*.	[CER]
	ST31-K330 and ST33-K8H0 secure microcontrollers - Power supply glitch detector characteristics, référence AN_31_GLITCH, version 2, mars 2013, *ST MICROELECTRONICS*.	[CER]
	ST31 – AIS31 Compliant Random Number user manual, référence UM_31_AIS31, version 2, février 2013, *ST MICROELECTRONICS*.	[CER]
	ST31 – AIS31 Reference Implementation – Start-up, online and total failure tests – Application Note, reference AN_31_AIS31, version 2, février 2013, *ST MICROELECTRONICS*.	[CER]

4. 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