Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance ANSSI-CC-2014/94-M01

Microcontrôleur sécurisé ST31-K330A révision H pour version bi-mode (contact et sans contact) ou version sans contact seulement, incluant optionnellement la librairie cryptographique Neslib v3.2, la librairie MIFARE DESFire EV1 v2.2 et la librairie MIFARE Plus-S v1.3

Certificat de référence : ANSSI-CC-2014/94

Paris, le 30 avril 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Microcontrôleur sécurisé ST31-K330A révision H pour version bi-mode (contact et sans contact) ou version sans contact seulement, incluant optionnellement la librairie cryptographique Neslib v3.2, la librairie MIFARE DESFire EV1 v2.2 et la librairie MIFARE Plus-S v1.3, 5 janvier 2015, ANSSI-CC-2014/94.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2014/94-S01, 21 août 2015.
[R-S02]	Rapport de surveillance ANSSI-CC-2014/94-S02, 7 septembre 2016.
[R-S03]	Rapport de surveillance ANSSI-CC-2014/94-S03, 18 janvier 2018.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	SECURITY IMPACT ANALYSIS REPORT – ST31-K330A Maskset K330A internal revision H including optional libraries Neslib 3.2, optional Mifare DESFire EV1 2.2 and optional Mifare Plus S 1.3, référence SMD_ST31K330A_revH__SIA_17_001, 21 février 2017, *STMICROELECTRONICS*.
[RM-Lab]	Evaluation Technical Report Addendum CHABLIS-2 Project, version 1.0, 30 mars 2017, référence Chablis-2_ETR_ADD_v1.0_copy2, *SERMA SAFETY & SECURITY*
[RA-Lab]	STMicroelectronics Development Environment - STM Tunis Site Visit Report (Full Report), version 1.0, 20 octobre 2017, référence 16-0227-STM-TNS_SVR_V1.0, *SERMA SAFETY & SECURITY*. STMicroelectronics Development Environment - STM Tunis Site Visit report (Lite Report), version 1.0, 20 octobre 2017, référence 16-0227-STM-TNS_SVR-M_V1.0, *SERMA SAFETY & SECURITY*.
[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 maintenu est le « Microcontrôleur sécurisé ST31-K330A révision H pour version bi-mode (contact et sans contact) ou version sans contact seulement, incluant optionnellement la librairie cryptographique Neslib v3.2, la librairie MIFARE DESFire EV1 v2.2 et la librairie MIFARE Plus-S v1.3 », développé par la société *STMICROELECTRONICS*. Il a été initialement certifié sous la référence ANSSI-CC-2014/94 (référence [CER]).

3. Description des évolutions

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

- retrait du cycle de vie du site :
  - *DISCO HI-TEC EUROPE GMBH*
    Liebigstrasse 8
    D-85551 Kirchheim bei München
    Allemagne

- ajout au cycle de vie du site :
  - *STMICROELECTRONICS*
    Cité Technologique des Communications
    BP21 2088 La Gazelle
    Tunisie

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [RM-Lab]) réévaluant les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit. Depuis ce rapport, l'audit du site *STMICROELECTRONICS* de Tunisie a été renouvelé (référence [RA-Lab]).

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]	*ST31 – K330 platform (Sx31Zxxx, Mx31Zxxx) – Datasheet*, référence DS_ST31-K330A, version 7, août 2016, *STMICROELECTRONICS*.	[R-S03]
	Application note – ST31-K330 security guidance, référence AN_SECU_ST31-K330, version 4, 5 septembre 2014, *STMICROELECTRONICS*.	[CER]
	Application note – ST31-K330 Dual interface secure microcontrollers - Recommendations for contactless operations, référence AN_31_RCMD, version 2, 28 juillet 2014, *STMICROELECTRONICS*.	[CER]
	ST31 NesLib cryptographic library - User manual, référence UM_31_NESLIB_3.2, version 7, 24 avril 2014, *STMICROELECTRONICS*.	[CER]
	ST31-K330 and ST33-K8H0 secure microcontrollers - Power supply glitch detector characteristics, référence AN_31_GLITCH, version 2, mars 2013, *STMICROELECTRONICS*.	[CER]
	MIFARE DESFire EV1 library 2.2 - user manual, reference UM_MIFARE_DESFire_EV1_2.2, version 4, avril 2015, *STMICROELECTRONICS*.	[R-S01]
	MIFARE DESFire EV1 interface specification User manual, référence UM_MIFARE_DESFire_EV1_Interface, version 5, décembre 2016, *STMICROELECTRONICS*.	[R-S03]
	MIFARE Plus S library 1.3 for ST31-K330 – User manual, référence UM_31_MIFARE_PLUS_S-1.3.0, 16 mai 2014, version 1, *STMICROELECTRONICS*.	[CER]
	MIFARE Plus S interface specification, référence UM_MIFARE_PLUS_S, version 1, octobre 2013, *STMICROELECTRONICS*.	[CER]
	ST31 – AIS31 Compliant Random Number user manual, référence UM_31_AIS31, version 2, février 2013, *STMICROELECTRONICS*.	[CER]
	ST31 – AIS31 Reference Implementation – Start-up, online and total failure tests – Application Note, référence AN_31_AIS31, version 2, février 2013, *STMICROELECTRONICS*.	[CER]
[ST]	*ST31 – K330A version H (dual or contactless mode only) with optional cryptographic library Neslib 3.2, and optional technology MIFARE DESFire EV1 2.2 and optional technology MIFARE Plus 1.3 - Security Target*, référence SMD_MR31Zxxx_ST_13_001, version 02.02, mars 2017, *STMICROELECTRONICS*.	[R-M01]

	ST31 – K330A version H (dual or contactless mode only) with optional cryptographic library Neslib 3.2, and with optional technology MIFARE DESFire EV1 2.2 and optional technology MIFARE Plus 1.3 Security Target – Public Version, référence SMD_MR31Zxxx_ST_13_002, version 02.03, mars 2017, *STMICROELECTRONICS*.	[R-M01]
[CONF]	ST31-K330 (SR31Z052) B02 – TOE References, version B02, *STMICROELECTRONICS*.	[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.

6. 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.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été 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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été 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 EAL4 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.org.
[2] Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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