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-2017/02-M01

Microcontrôleurs sécurisés ST33G1M2A et ST33G1M2M révision G, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 4.2.10

Certificat de référence : ANSSI-CC-2017/02

Paris, le 11 janvier 2019

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Microcontrôleurs sécurisés ST33G1M2A et ST33G1M2M révision G, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 4.2.10, 16 février 2017, ANSSI-CC-2017/02.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2017/02-S01, 28 décembre 2018.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Impact analysis report – Evaluation for ST33GM2x rev G, référence SMD_33G_SIA_18_001, version 1.01, 7 mars 2018.
[RM-Lab]	Evaluation Technical Report – Project : ST33G1M2A/ST33G1M2M Surveillance 2018, 30 mars 2018, LATAM_Surv2018_ETR, version 1.0, *THALES*.
[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 « Microcontrôleurs sécurisés ST33G1M2A et ST33G1M2M révision G, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 4.2.10 », développé par la société *ST MICROELECTRONICS* et initialement certifié sous la référence ANSSI-CC-2017/02 (référence [CER]).

3. Description des évolutions

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

Opération	Identification du site
Renommage d'un site existant	WINSTEK (au lieu de *STATS CHIPPAC* (SCT)) No 176-5, 6 Lane, Hualung Chun, Chiung Lin, 307 Hsinchu, Taiwan
Ajout au cycle de vie	*JCET STATSCHIPPAC* (JSCC) N°78 Changshan Road, Jiangyin, Jiangsu, 214437, Chine
Retrait du cycle de vie	*NEDCARD* Bijsterhuizen 25-29, 6604 LM Wijchen, Pays-Bas
	STMICROELETRONICS 18 Ang Mo Kio Industrial park, 569505 Singapour, Singapour

	STATS CHIPPAC (SCC) 188 Huaxu Rd, Qingpu district, 201702 Shanghaï, Chine
	STMICROELECTRONICS Sdn. Bhd. Tanjong Agas, Industrial area. P.o. Box 28, 84007 Muar, Johor, Malaisie

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]	ST33G Platform - ST33G1M2A: Automotive-grade secure MCU with 23-bit Arm SecurCore SC300 CPU and high-density Flash memory – Datasheet, reference: DS_ST33G1M2A, revision 2, December 2017.	[R-S01]
	ST33G Platform - ST33G1M2M: M2M industrial secure MCU with 32-bit Arm SecurCore SC300 CPU and high density Flash memory – Datasheet, reference: DS_ST33G1M2M, revision 3, January 2018.	[R-S01]
	ST33G1M2A, ST33G1M2M: CMOS M10+ 80nm technology die and wafer delivery description, reference DD_ST33G1M2A_M, revision 4, October 2016.	[CER]
	ST33 uniform timing application note, reference: AN_33_UT revision 2, November 2013.	[CER]
	ST33G1M2A/ST33G1M2M firmware User Manual, reference UM_ST33G1M2A_M_FW, revision 8, January 2018.	[R-S01]
	ST33G and ST33H Firmware support for LPU regions – Application note, reference AN_33G_33H_LPU, revision 1, March 2014.	[CER]
	ST33G and ST33H Security Guidance, reference AN_SECU_ST33, revision 5.0, February 2016.	[CER]
	ST33G and ST33H Power supply glitch detector characteristics - Application Note, reference AN_33_GLITCH, revision 2.0, January 2014.	[CER]
	ST33G and ST33H - AIS31 Compliant Random Number user manual, reference UM_33G_33H_AIS31, revision 3, October 2015.	[CER]

	ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, reference AN_33G_33H_AIS31, revision 1, October 2013.	[CER]
	ARM Execute-only memory support for ST3x Secure microcontrollers based on SecurCore SC000 and SC300 devices - Application Note, reference AN_33_EXE, revision 2, November 2014.	[CER]
	NesLib 4.2 Library, User manual, reference UM_NESLIB_4.2, revision 1, July 2015.	[CER]
	NesLib 4.2 for ST33 platforms – Release note, reference RN_ST33_NesLib4.2.10, revision 4, January 2017.	[CER]
	ST33G and ST33H Secure MCU platforms NesLib 4.2 security recommendations, reference AN_SECU_ST33_NESLIB_4.2, revision 2, October 2015.	[CER]
	Flash memory loader installation guide for ST33G1M2A and ST33G1M2M platforms, reference UM_33GA_FL_v3, revision 3, August 2016.	[CER]
[ST]	ST33G platform ST33G1M2A, ST33G1M2M, maskset K8H0A version G, with firmware revision 1.3.2, optional cryptographic library Neslib 4.2.10 SECURITY TARGET, reference SMD_ST33G_ST_14_001_v01.09, revision 1.09, March 2018.	[R-M01]
	ST33G platform ST33G1M2A, ST33G1M2M, maskset K8H0A version G, with firmware revision 1.3.2, optional cryptographic library Neslib 4.2.10 Security Target for composition, reference SMD_ST33G_ST_16_001_v1.04, revision v1.04, March 2018.	[R-M01]
[CONF]	ST33G1M2A, ST33G1MEM & derivatives (HW rev G, FW 1.3.2 and optional NesLib 4.2.10) - CONFIGURATION LIST, reference SMD_33G_CFGL_16_001, revision 1.02, March 2018.	[R-M01]
	ST33G1M2A, ST33G1MEM and derivatives CC EAL 5+ Project Evaluation (HW rev G, FW 1.3.2 and optional NesLib 4.2.10) - DOCUMENTATION REPORT, reference SMD_ST33G1M2AM_DR_16_001_v01.04, revision 1.04.	[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. 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)

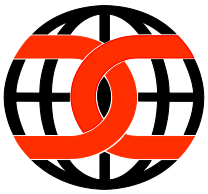
Le certificat initial a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

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 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.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