



**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-2017/73-M01

ST33G1M2A1 B03

Certificat de référence : ANSSI-CC-2017/73

Paris, le 8 octobre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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

La reproduction de ce document sans altération ni coupure est autorisée.

1 Références

[CER]	Rapport de certification ANSSI-CC-2017/73, Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique NesLib 6.0.3 et la bibliothèque SFM 1.0.7, 18 décembre 2017.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2017/73-S01, Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique NesLib 6.0.3 et la bibliothèque SFM 1.0.7, 18 octobre 2019.
[IAR]	Security Impact Analysis Report – ST33G1M2A1 B03, version SMD_ST33G1M2A1_B03_SIA_20_001, révision 1.0, 24 septembre 2020.
[RM-Lab]	Partial Evaluation Technical Report Project: ST33G1M2A1 B03 Maintenance, référence: LATOURAM2_B03_Maintenance_ETR, révision: 1.0 , 5 octobre 2020
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</i>
[CCRA]	<i>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.</i>

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « ST33G1M2A1 B03 » développé par la société STMicroelectronics. ST33G1M2A1 B03 correspond au microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique NesLib 6.0.3 et la bibliothèque SFM 1.0.8. (référence [ST]).

Le produit « ST33G1M2A1 » a été initialement certifié sous la référence ANSSI-CC-2017/73 (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 la librairie SFM de la version 1.0.7 à la version 1.0.8 pour correction de bugs fonctionnels liés à l'activation de la fonctionnalité de répartition de l'usure de la mémoire (« *wear-leveling* ») et à la fonction de défragmentation de la mémoire ;
- mise à jour de la liste des sites du cycle de vie.

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]	ST33G1M2A: Automotive-grade secure MCU with 32-bit ARM SecurCore SC300 CPU and high-density Flash memory Datasheet, DS_ST33G1M2A Rev 3, mai 2018 ;	[R-S01]
	ST33G1M2A Firmware - User manual, UM_ST33G1M2A_M_FW Rev 11, février 2019 ;	[R-S01]
	NesLib cryptographic library NesLib 6.0 - User manual, UM_NesLib_6.0 Rev 2, mars 2017 ;	[R-S01]
	ST33 Secure MCU platforms NesLib 6.0 security recommendations - Application note, AN_SECU_ST33_NESLIB_6.0 Rev 3, septembre 2019 ;	[R-S01]
	NesLib 6.0.3 for ST33 platforms - Release note, RN_ST33_NESLIB_6.0.3 Rev 4, juillet 2019 ;	[R-S01]
	StoreKeeper v1.0 - User manual, UM_StoreKeeper Rev 3, novembre 2016 ;	[CER]
	Security recommendation Application Note SFM Library 1.0, AN_SECU_StoreKeeper Rev 1, Janvier 2017 ;	[CER]
	ST33G and ST33H - AIS31 Compliant Random Number - User Manual, UM_33G_33H_AIS31 Rev 3, octobre 2015 ;	[CER]
	ST33G and ST33H - AIS31 - Ref. impl.: Start-up, on-line and total failure tests - Application note, AN_33G_33H_AIS31 Rev 1, octobre 2013 ;	[CER]
	ST33G and ST33H Secure MCU platforms - Security Guidance, AN_SECU_ST33 Rev 8, mai 2019 ;	[R-S01]
	User manual : Blackbox project – Developpeur Kit system overview, référence OPE_UG_09_001, révision 2.02, août 2013 ;	[CER]
	Datasheet : BlackBox – ST BlackBox interface, référence DS_BLACKBOX, révision 2, octobre 2012.	[CER]
	Flash memory loader installation guide for the ST33G1M2A and ST33G1M2M platforms, UM_33GA_FL Rev 3, août 2016.	[CER]
[ST]	<p>Cibles de sécurité de référence:</p> <p>ST33G platform ST33G1M2A1 maskset K8H0A version H, with firmware revision 1.3.2, optional cryptographic library NesLib 6.0.3, and optional library SFM 1.0.8, Security Target, SMD_ST33G_ST_16_001 Rev 1.08, septembre 2020 ;</p> <p>Version publique : .</p> <p>ST33G platform ST33G1M2A1 maskset K8H0A version H, with firmware revision 1.3.2, optional cryptographic library NesLib 6.0.3, and optional library SFM 1.0.8 Security Target For Composition, SMD_ST33G_ST_16_002 Rev 1.07, septembre 2020.</p>	[R-M01]
[CONF]	ST33G1M2A1 B03 including optional cryptographic library NesLib 6.0.3, and optional library SFM 1.0.8 Configuration List, SMD_33G_CFGL_16_002, rev 1.0, septembre 2020.	[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'accord¹, 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 signataires², 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.