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-2014/46-M01

Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et 4.1.1 et la bibliothèque MIFARE® DESFire® EV1 révision 3.7 ou 3.8

Certificat de référence : ANSSI-CC-2014/46

Paris, le 17 mars 2016

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 ST33G1M2 révision F, Firmware révision 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE® DESFire® EV1 révision 3.7 ou 3.8, 21 juillet 2014, ANSSI-CC-2014/46.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2014/46-S01, 20 octobre 2015.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR1]	ImpactAnalysis Report – Evolutions on ST33G Platforms, reference SMD_33G_SIA_15_001, 27 July 2015, STMicroelectronics.
[IAR2]	ImpactAnalysis Report – Update on ST33G & ST33H Platforms, reference SMD_33_SIA_15_001, 21 Oct. 2015, STMicroelectronics.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, juillet 2014.

2. Identification du produit maintenu

Le produit maintenu est le « Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et 4.1.1 et la bibliothèque MIFARE® DESFire® EV1 révision 3.7 ou 3.8 » développé par *STMICROELECTRONICS*.

Le produit « Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révisions 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE® DESFire® EV1 révision 3.7 ou 3.8 » a été initialement certifié sous la référence ANSSI-CC-2014/46 (référence [CER]).

La version maintenue du produit est identifiable par les éléments suivants (voir [ST] au paragraphe 3.1 « TOE identification » et [GUIDES]) :

- informations obtenues avec la la méthode « Get Product Information » tel que documenté dans le « Firmware User Manual » (voir [GUIDES]) :
  - identifiant du produit : l'API retourne le *Master ID* qui est l'identifiant du produit maître (valeur **0061**h pour du produit ST33G1M2 et valeur **0105**h pour la version améliorée ST33I1M2 du produit ST33G1M2) ;
  - **09**h ou **0A**h : version interne du *firmware*, valeur en hexadécimal écrite sur un octet ;
- informations obtenues avec la commande « NesLib_GetVersion » (voir [GUIDES] pour la description de l'API) :
  - **1410**h : référence de la bibliothèque cryptographique NesLib version 4.1 ;
  - **1411**h : référence de la bibliothèque cryptographique NesLib version 4.1.1.

3. Description des évolutions

Les rapports d'analyse d'impact de sécurité (références [IAR1] et [IAR2]) mentionnent que les modifications suivantes ont été opérées :

- une nouvelle version 4.1.1 de la bibliothèque cryptographique NesLib optimisée en taille peut être embarquée sur le produit ;
- l'amélioration de la performance du produit pour la version ST33I1M2 ;
- une erreur fonctionnelle mineure a été corrigée dans le *firmware* du produit.

4. Fournitures applicables

Les fournitures, notamment les guides applicables du produit évalué, sont applicables au produit maintenu et sont listés dans le tableau ci-dessous. 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.

Les guides contenant de nouvelles recommandations sécuritaires obligatoires par rapport au certificat initial apparaissent en gras.

[GUIDES]	ST33G Platform - ST33G1M2: Secure MCU with 32-bit ARM® SecurCore® SC300TM CPU and high density Flash memory – Datasheet, reference: DS_33G1M2, revision 3, May 2014.	[CER]
	ST33G1M2 family extension – Technical note, reference TN_ST33G1M2_03, revision 1, July 2015.	[R-M01]
	ST33 uniform timing application note, reference: AN_33_UT revision 2, November 2013.	[CER]
	ST33G1M2 Firmware User Manual, reference UM_ST33G1M2_FW, revision 6, May 2014.	[CER]
	ST33G and ST33H Security Guidance, reference: AN_SECU_ST33, revision 3.0, March 2015.	[R-S01]
	ST33G and ST33H - AIS31 Compliant Random Number user manual, reference UM_33G_33H_AIS31, revision 2, February 2014.	[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]
	ST33 NesLib Library User manual, NesLib 4.1 and 4.1.1 for ST33 Secure MCUs, reference UM_33_NESLIB_4, revision 4, December 2014.	[R-M01]
	ST33 Secure MCU family NesLib 4.1 and NesLib 4.1.1 security recommendations, reference AN_SECU_33_NESLIB_4, revision 7, April 2015.	[R-S01]
	MIFARE® DESFire® EV1 Library 3.7 for ST33G1M2 Secure MCUs – User Manual, reference UM_MIFARE_DESFire-EV1-3.7, revision 2, February 2013.	[CER]
	MIFARE® DESFire® EV1 Library 3.8 for ST33G1M2 Secure MCUs – User Manual, reference UM_MIFARE_DESFire-EV1-3.8, revision 1, April 2013.	[CER]

	ST33G1M2 and derivatives – Flash loader installation guide, reference UM_33G_FL_v4, revision 4, August 2015.	[R-M01]
[ST]	Cible de sécurité de référence pour l'évaluation : - ST33G1M2 platform version F with firmware revision 9 and A, optional cryptographic library Neslib 4.1 and 4.1.1, and optional technology MIFARE® DESFire® EV1 3.7 & 3.8 – Security Target, reference SMD_ST33G_ST_13_001_v3.04, revision 3.04, October 2015. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST31G1M2 platform version F with firmware revision 9 and A, optional cryptographic library Neslib 4.1 and 4.1.1, and optional technology MIFARE® DESFire® EV1 3.7 & 3.8 – Security Target, reference SMD_ST33G_ST_13_002_v2.5, revision v2.05, October 2015.	[R-M01]
[CONF]	Liste de configuration : - ST33G1M2 rev F & derivatives (incl. Firmware rev 9 and rev A, optional NesLib v4.1 & v4.1.1, MIFARE Classic v1.3, MIFARE® DESFire® EV1 v3.7 & v3.8) CONFIGURATION LIST, reference SMD_33G_CFGL_13_001_v2.1, revision 1.0, October 2015. Liste de la documentation : - ST33G1M2 rev F & derivatives (incl. Firmware rev 9 and rev A, optional NesLib v4.1 and v4.1.1, MIFARE Classic v1.3, MIFARE® DESFire® EV1 v3.7 & v3.8) DOC REPORT, reference SMD_ST33G1M2_DR_13_001_v01.06, revision 1.06, October 2015.	[R-M01]
[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 : - Evaluation Technical Report for composite evaluation, Project LATOUR, reference Maint_LAT_ETRLite, révision 1.0, 2 December 2015, Thales.	[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, à la date de certification.
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 la 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 :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], 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] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.