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-2017/01-M01

Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 5, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile version 2.1.0

Certificat de référence : ANSSI-CC-2017/01

Paris, le 10 juillet 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 5, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile version 2.1.0, 10 février 2017, ANSSI-CC-2017/01.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2017/01-S01, 30 avril 2018.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	IMPACT ANALYSIS REPORT – Development Environment Evolution on ST33H768 Platform, version 1.00, 6 mars 2017, référence SMD_ST33H768_SIA_17_001.
[R-Lab]	Evaluation Technical Report Project ST33H768, version 2.0, 20 avril 2018, LAT2_ETR, *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 « Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 5, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile version 2.1.0 », développé par la société *STMICROELECTRONICS*.

Ce produit a été initialement certifié sous la référence ANSSI-CC-2017/01 (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 des sites suivants :
  - *DISCO HI-TEC EUROPE GMBH*
    Liebigstrasse 8
    D-85551 Kirchheim bei München
    Allemagne

  - *NEDCARD*
    Bijsterhuizen 25-29
    6604 LM Wijchen
    Pays-Bas

Le CESTI en charge de l'évaluation initiale a émis un rapport d'évaluation partielle (référence [R-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]	ST33H Platform - ST33H768: Secure MCU with 32-bit ARM SecurCore SC300 CPU - and high density Flash memory – Datasheet, reference: DS_ST33H768, revision 4, April 2015.	[CER]
	ST33H768: BP and BM specific product profiles – Technical, note, reference TN_ST33H768_01, revision 1, April 2015.	[CER]
	ST33H768: LS, LC and BS specific product profiles – Technical, note, reference TN_ ST33H768_02, revision 1, April 2015.	[CER]
	ST33H768 : CMOS M10+ 80nm technology die and wafer delivery description, reference DD_ST33H768, revision 2, March 2014	[CER]

	ST33 uniform timing application note, reference: AN_33_UT, revision 2, November 2013.	[CER]
	ST33H768 Firmware User Manual, reference UM_ST33H768_FW, revision 5, May 2015.	[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]
	ST33 ARM Execute-only memory support for SecurCore SC300 devices - Application Note, reference AN_33_EXE, revision 2, November 2014.	[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.	[CER]
	NesLib 4.1 for ST33 – Limitations versus NesLib 4.1.1, reference TN_ST33G_NesLib4.1, revision 4, July 2015 .	[CER]
	ST33 Secure MCU family NesLib 4.1 and NesLib 4.1.1 security recommendations, reference AN_SECU_33_NESLIB_4, revision 7, April 2015.	[CER]
	ST33H and derivatives – Flash loader installation guide, reference UM_33H_FL_v4, revision 4, August 2015.	[CER]
	MIFARE4Mobile Library 2.1 – User Manual, reference UM_MIFARE4Mobile-2.1, revision 5, June 2015.	[CER]
	MIFARE4Mobile Library 2.1 for ST33G1M2 – Application note, reference AN_ST33G1M2_M4M_Lib, revision 1, June 2015.	[CER]

[ST]	Cibles de sécurité de référence: - ST33H768 platform maskset K8K0A version C, with firmware revision 5, optional cryptographic library Neslib 4.1 and 4.1.1, and optional technology MIFARE4Mobile 2.1.0 – Security target, reference SMD_ST33H_ST_16_001_V01.04, revision 1.04, March 2017 ; Version publique - ST33H768 platform maskset K8K0A version C with firmware revision 5, and optional cryptographic library Neslib 4.1 and 4.1.1, and optional technology MIFARE4Mobile 2.1.0 – Security Target for composition, reference SMD_ST33H_ST_16_002, revision 1.01, March 2017.	[R-M01]
[CONF]	ST33H768 rev C & derivatives (incl. Firmware rev 5, optional NesLib 4.1 and 4.1.1 MIFAE4Mobile v2.1.0) CONFIGURATION LIST, reference SMD_ST33H_CFGL_16_001, revision 1.02, September 2016.	[CER]
	ST33H768 and Derivatives CC EAL 5+ Project Evaluation (including FW rev 5, opt. Neslib v4.1 and v4.1.1, opt. MIFARE M4M v2.1.0) - DOCUMENTATION REPORT, reference SMD_ST33H768_DR_17_001_v01.07, revision 1.07.	[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