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-2016/58-M02

ST31G480 A04 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X

Certificat de référence : ANSSI-CC-2016/58

Paris, le 16 juin 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Rapport de certification ANSSI-CC-2016/58, ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X, 25 août 2016, ANSSI.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2016/58-M01, ST31G480 A03 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X, 10 février 2017.
[IAR]	Security impact analysis report, ST31G480 Maskset K8L0B revision H (TOE rev A04), SMD_ST31G480_A04_SIA_17_001, 30 mars 2017, 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, 2 juillet 2014.

2. Identification du produit maintenu

Le produit ST31G480 A02, a été initialement certifié sous la référence ANSSI-CC-2016/58 (référence [CER]).

Il a déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2016/58-M01 (référence [R-M01]).

Le produit objet de la présente maintenance est ST31G480 A04 développé par la société STMICROELECTRONICS.

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

- IC Maskset name : K8L0B ;
- IC version : H ;
- Master product identification number : 00B8 ;
- Firmware version : 2.1.0 ;
- OST version : 3.4 ;
- (optionnel) NesLib crypto library version : 4.2.10 ;
- (optionnel) MIFARE DESFire EV1 version : 4.8.12 ;
- (optionnel) MIFARE Plus X version : 2.4.6.

Toutes ces valeurs sont disponibles à travers les interfaces logiques du produit, selon les méthodes et formats décrits dans [GUIDES]. De plus, « K8L0B » (valeur IC Maskset name) est gravée sur la surface du composant.

3. Description des évolutions

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

- Correction d'un *bug* fonctionnel de MIFARE DESFire EV1, donnant lieu à la version 4.8.12 ;
- Modification du guide « MIFARE DESFire EV1 library 4.8.12 for ST31G480 – Application note » de référence AN_ST31G480_MFD_Lib.

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-M02] référence la présente maintenance.

[GUIDES]	ST31G platform ST31G480, Datasheet – preliminary data, DS_ST31G480 Rev 2, décembre 2016, STMICROELECTRONICS.	[R-M01]
	ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, septembre 2010, ARM.	[CER]
	ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, septembre 2010, ARM.	[CER]
	ST31G and ST31H Secure MCU platforms, Security guidance, AN_SECU_ST31G_H Rev 3, mars 2016, STMICROELECTRONICS.	[CER]
	ST31 firmware, User manual, UM_ST31_FW Rev 9, mars 2016, STMICROELECTRONICS.	[CER]
	NesLib 4.2 library, User manual, UM_NESLIB_4.2 Rev 1.0, juillet 2015, STMICROELECTRONICS.	[CER]
	ST31G and ST31H Secure MCU platforms NesLib 4.2 security recommendations, AN_SECU_ST31_NESLIB_4.2 Rev1, août 2015, STMICROELECTRONICS.	[CER]
	NesLib 4.2.10 for ST31 platforms, release note, RN_ST31_NESLIB_4.2.10 Rev 4, janvier 2016, STMICROELECTRONICS.	[CER]
	ST31G480 Flash memory loader installation guide, User manual, UM_31G_FL Rev2, février 2016, STMICROELECTRONICS.	[CER]
	ST31G and ST31H - AIS31 Compliant Random Number - User Manual, UM_31G_31H_AIS31 Rev 1.0, janvier 2015, STMICROELECTRONICS.	[CER]
	ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, AN_31G_31H_AIS31 Rev 1, janvier 2015, STMICROELECTRONICS.	[R-M01]
	MIFARE DESFire EV1 library 4.8 for ST31G480 secure microcontrollers, User Manual, UM_31_MFDF_EV1_4.8 Rev 4, février 2016, STMICROELECTRONICS.	[CER]
	MIFARE DESFire EV1 library 4.8.12 for ST31G480 –Application note, AN_ST31G480_MFD_Lib Rev 3.0, mars 2017, STMICROELECTRONICS.	[R-M02]
	MIFARE DESFire EV1 Interface Specification, User Manual, UM_Mifare_Desfire_EV1_Interface, Rev 4.0, avril 2016, STMICROELECTRONICS.	[CER]

	MIFARE Plus X library 2.4 for ST31G480- User Manual, UM_MIFARE_PLUS_X_2_4 Rev 5, février 2016, STMICROELECTRONICS.	[R-M01]
	Application note, Mifare Plus X library 2.4.6 for ST31G480, AN_ST31G480_MFP-X_Lib Rev 1.0, décembre 2016, STMICROELECTRONICS.	[R-M01]
[ST]	Cible de sécurité de référence pour la maintenance : - ST31G480 A04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target, SMD_ST31G480_ST_14_001 Rev A04.1, avril 2017, STMICROELECTRONICS. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette maintenance : - ST31G480 A04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target for composition, SMD_ST31G480_ST_14_002 Rev A04.1, avril 2017, STMICROELECTRONICS.	[R-M02]
[CONF]	ST31G480 A04 – TOE References, avril 2017, STMICROELECTRONICS	[R-M02]

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 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 :

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

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, l'Ethiopie, 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, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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