



**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-2019/12-M02

ST31G480

D04

Certificat de référence : ANSSI-CC-2019/12

Paris le 18 juillet 2022

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

Guillaume POUPARD

[ORIGIANL 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-2019/12, ST31G480 D01, 5 mars 2019.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2019/12-S01, ST31G480 D02, 23 juillet 2020.
[R-S02]	Rapport de surveillance ANSSI-CC-2019/12-S02, ST31G480 D03, 26 juillet 2021.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01
[R-M01]	Rapport de maintenance ANSSI-CC-2019/12-M01, ST31G480 D03, 26 juillet 2021.
[IAR]	Security impact analysis report, ST31G480 D04, ST31G480_D04_SIA, avril 2022.
[RM-Lab]	Surveillance Technical Report – Elixir3 & Elixir4 projet, Elixir3_D03_Elixir4_E03_STR_v1.1, 7 juillet 2021, SERMA SAFETY & SECURITY.
[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 « ST31G480, D04 » développé par la société STMICROELECTRONICS.

Le produit « ST31G480, D01 » a été initialement certifié sous la référence ANSSI-CC-2019/12 (référence [CER]).

Il a déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2019/12-M01 (référence [R-M01]).

3 Description des évolutions

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

- clarification de la taille minimale des clés RSA dans la cible de sécurité ;
- prise en compte de la nouvelle adresse du site SmartFlex.

Le CESTI en charge de l'évaluation initiale a émis un rapport (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-M02] référence de la présente maintenance.

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

[GUIDES]	<i>ST31G Platform - ST31G480 - Datasheet – production data, DS_ST31G480, Rev 4, 13 avril 2018</i>	[CER]
	<i>ARM Cortex SC000 Technical Reference Manual, ARM DDI 0456, issue A, septembre 2010</i>	[CER]
	<i>ARMv6-M Architecture Reference Manual, ARM DDI 0419, issue C, septembre 2017</i>	[CER]
	<i>ST31 Firmware User Manual, UM_ST31_FW, Rev 10, juin 2019</i>	[R-S02]
	<i>ST31G480 Flash loader installation guide - User manual, UM_31G_FL, Rev 2, février 2016</i>	[CER]
	<i>NesLib 6.2 library - User manual, UM_NesLib_6.2, Rev 3, mars 2020</i>	[R-S01]
	<i>ST31G and ST31H Secure MCU family - NesLib 6.2 security recommendations, Application Note AN_SECU_ST31G_H_NESLIB_6.2, Rev 8, septembre 2019</i>	[R-S01]
	<i>Release note Neslib 6.2.1 for the ST31G and ST31H platforms, RN_ST31_NESLIB_6.2.1, Rev 6, mars 2020</i>	[R-S01]
	<i>ST31G and ST31H Secure MCU platforms Security Guidance, Application note AN_SECU_ST31G_H, Rev 10, avril 2021</i>	[R-S02]
	<i>ST31G and ST31H - AIS31 Compliant Random Number User Manual, UM_31G_31H_AIS31, Rev 1, janvier 2015</i>	[CER]
	<i>ST31 - AIS31 Reference implementation - Startup online and total failure tests - Application Note, AN_31G_31H_AIS31, Rev 1, janvier 2015</i>	[CER]
	<i>MIFARE DESFire EV1 library 4.8 for ST31G480 - User manual, UM_31_MFDF_EV1_4.8, Rev 4, février 2016</i>	[CER]
	<i>MIFARE DESFire EV1 library 4.8.12 for ST31G480 - Appli note, AN_ST31G480_MFD_Lib, Rev 3, mars 2017</i>	[CER]
	<i>MIFARE DESFIRE EV1 interface specification User manual, UM_Mifare_Desfire_EV1_Interface, Rev 5, décembre 2016</i>	[CER]
	<i>MIFARE Plus X library 2.4 for ST31G480 - User manual, UM_MIFARE_PLUS_X_2_4, Rev 5, décembre 2016</i>	[CER]
	<i>MIFARE Plus X library 2.4.6 for ST31G480 - Application note, AN_ST31G480_MFPX_Lib, Rev 1, décembre 2016</i>	[CER]
	<i>MIFARE Plus X and MIFARE Plus EV1 IV manipulation attack and mitigations, Technical note TN_MFP_IV Rev 1, avril 2020</i>	[R-S01]

[ST]	<i>ST31G480 D04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X, Security Target for composition, SMD_ST31G480_ST_17_003 rev D04.0, avril 2022</i>	[R-M02]
[CONF]	<i>ST31-K8L0-Configuration List -D04, SMD_ST31G480_TOE_Ref_D04 rev D04, avril 2022</i>	[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 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.

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.

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 :

