



**PREMIÈRE
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-2020/30-M01

ST33J2M0 D03

Certificat de référence : ANSSI-CC-2020/30

Paris le 12 Décembre 2022

Le Directeur général adjoint de l'Agence
nationale de sécurité des systèmes d'information

Emmanuel NAEGELEN

[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-2020/30, ST33J2M0 D01 including optional cryptographic library NESLIB and optional technology MIFARE4Mobile, 9 juillet 2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2020/30-S01, ST33J2M0 D02, 15 janvier 2021.
[R-S02]	Rapport de surveillance ANSSI-CC-2020/30-S02, ST33J2M0 D02, 22 octobre 2021
[R-S03]	Rapport de surveillance ANSSI-CC-2020/30-S03, ST33J2M0 D03.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	<i>Security Impact Analysis report – ST33J A06 C02 D03</i> , référence SMD_ST33J_A06_C02_D03_SIA_22_001_v1_1, version 1.1, 25 juillet 2022.
[RM-Lab]	<i>Surveillance Technical Report - PERCEVAL A06, C02 and D03 Project</i> , référenec PERCEVAL_A06_C02_D03_STR_v1.1, version 1.1, 14 octobre 2022.
[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 « ST33J2M0 D03 » développé par la société STMICROELECTRONICS.

Le produit « ST33J2M0 D01 including optional cryptographic library NESLIB and optional technology MIFARE4Mobile » a été initialement certifié sous la référence ANSSI-CC-2020/30 (référence [CER]).

3 Description des évolutions

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

- correction des adresses de sites de STMICROELECTRONICS du cycle de vie du produit décrit dans la cible de sécurité ;
- changement d'adresse du site de STMICROELECTRONICS Sophia ;
- clarification de la taille minimale des clés RSA dans la cible de sécurité [ST].

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]	<i>ST33J2M0 Datasheet, référence DS_ST33J2M0, version 9, avril 2020.</i>	[R-S01]
	<i>User manual ST33J2M0 firmware V3, référence UM_ST33J2M0_FWv3, version 20, mai 2020.</i>	[R-S01]
	<i>Application note ST33J Secure MCU platform Security guidance, référence AN_SECU_ST33J, version 10, décembre 2019.</i>	[CER]
	<i>ARM® SC300 r0p1 Technical reference Manual, référence ARM_DDI_0447, version A, 24 juin 2009.</i>	[CER]
	<i>ARM® Cortex-M3 r2p0 Technical Reference Manual, référence ARM_DDI_0037F3c, version F3c, 31 janvier 2008.</i>	[CER]
	<i>ARM® SecurCore SC300 (AT500) Product Errata Notice, référence PR326-PRDC-009983, version 11, 24 février 2015.</i>	[CER]
	<i>User manual, ST33J platform - AIS 31, compliant random number, référence UM_ST33J_AIS31, version 1, mai 2016.</i>	[CER]
	<i>ST33J platform AIS31 – Application note, reference implementation: Start-up, on-line and total failure tests, référence AN_ST33J_AIS1, version 1, mai 2016.</i>	[CER]
	<i>MIFARE4Mobile library 2.2 for the ST33J platform - User manual, référence UM_33J_MIFARE4MOBILE-2.2, version 4, octobre 2016.</i>	[CER]
	<i>MIFARE4Mobile library 2.2.9 for the ST33J platform - Application note, référence AN_ST33J_M4M_Lib, version 1, octobre 2016.</i>	[CER]
	<i>MIFARE4Mobile library 2.2.10 for the ST33J platform - Application note, référence AN_ST33J_M4M_Lib, version 2 octobre 2016..</i>	[CER]
	<i>User manual – NesLib cryptographic library NesLib 6.3, référence UM_NesLib_6.3 version 4, 18 juillet 2019.</i>	[CER]
	<i>Application Note – ST33J secure MCU platforms – NesLib 6.3 security recommendations, référence AN_SECU_ST33J_NESLIB_6.3, version 5, juin 2022.</i>	[R-S03]
	<i>Neslib 6.3.4 for ST33 Lockstep platform - Release note, référence RN_ST33J_NESLIB_6.3.4, version 4, juillet 2022.</i>	[R-S03]
[ST]	Cibles de sécurité de référence: <ul style="list-style-type: none"> - <i>ST33J2M0 D03 including optional cryptographic library NESLIB and optional technology MIFARE4Mobile® Security Target, référence SMD_ST33J2M0_ST_19_003, version D03.0, Juillet 2022.</i> 	[R-M01]

	Version publique : . <ul style="list-style-type: none"> - <i>ST33J2M0 D03 including optional cryptographic library NESLIB and optional technology MIFARE4Mobile® Security Target for composition</i>, référence SMD_ST33J2M0_ST_19_004, version D03.0, Juillet 2022. 	
[CONF]	<ul style="list-style-type: none"> - <i>ST33J2M0 D03 – HW Rev H - CONFIGURATION LIST</i>, référence SMD_33J2M0_D03_CFGL_22_001, version 1.0, Août 2022. - <i>ST33J2M0 D03 – HW Rev I - CONFIGURATION LIST</i>, référence SMD_33J2M0_D03_CFGL_22_002, version 1.0, Août 2022. 	[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 :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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 :



² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.