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-2017/60-M01

ST31H320 B02 including optional cryptographic library NESLIB

Certificat de référence : ANSSI-CC-2017/60

Paris, le 6 juillet 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2017/60, ST31H320 B01 including optional cryptographic library NESLIB, 5 octobre 2017.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Security Impact Analysis Report, SMD_ST31H320_B02_SIA_18_001, 26 avril 2018, *STMICROELECTRONICS*.
[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 ST31H320 B01 a été initialement certifié sous la référence ANSSI-CC-2017/60 (référence [CER]).

Le produit objet de la présente maintenance est ST31H320 B02 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 : K8N0A ;
- IC version : E ;
- Master product identification number : 00DE ;
- Firmware version : 3.0.1 ;
- OST version : 4.0 ;
- (optionnel) NesLib crypto library version : 4.2.10 ou 5.2.0.

Toutes ces valeurs sont disponibles à travers les interfaces logiques du produit, selon les méthodes et formats décrits dans [GUIDES].

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :
- modification du logiciel dédié Firmware (désormais version 3.0.1) pour correction de bugs ;
- mise à jour du guide utilisateur UM_ST31G_H_FWv3 : alignement avec la nouvelle version de Firmware, clarifications.

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]	ST31H platform ST31H320, Datasheet – production data, DS_ST31H320 Rev 2, janvier 2016	[CER]
	ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, septembre 2010	[CER]
	ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, septembre 2010	[CER]
	ST31 firmware V3, User manual, UM_ST31G_H_FWv3 Rev 6, février 2018	[R-M01]
	NesLib 4.2 library, User manual, UM_NESLIB_4.2 Rev 1.0, juillet 2015	[CER]
	ST31G and ST31H Secure MCU platforms NesLib 4.2 security recommendations, AN_SECU_ST31_NESLIB_4.2 Rev1, août 2015	[CER]
	NesLib 4.2.10 for ST31 platforms, release note, RN_ST31_NESLIB_4.2.10 Rev 4, janvier 2016	[CER]
	NesLib cryptographic library NesLib 5.2, User manual, UM_NesLib_5.2 Rev2, juillet 2016	[CER]
	ST31G and ST31H Secure MCU platforms NesLib 5.2 security recommendations, Application note, AN_SECU_ST31_NESLIB_5.2 Rev 3, décembre 2016	[CER]
	NesLib 5.2.0 for ST31 platforms, Release note, RN_ST31_NESLIB_5.2.0 Rev 3, juin 2017	[CER]
	ST31G and ST31H Secure MCU platforms, Security guidance, AN_SECU_ST31G_H Rev 4, novembre 2016	[CER]
	ST31G and ST31H - AIS31 Compliant Random Number - User Manual, UM_31G_31H_AIS31 Rev 1.0, janvier 2015	[CER]
	ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, AN_31G_31H_AIS31 Rev 1, janvier 2015	[CER]
[ST]	Cible de sécurité de référence pour la maintenance : - ST31H320 B02 including optional cryptographic library NESLIB, Security Target, SMD_ST31H320_ST_17_001 Rev B02.1, février 2018. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette maintenance : - ST31H320 B02 including optional cryptographic library NESLIB, Security Target for composition, SMD_ST31H320_ST_17_002 Rev B02.1, février 2018.	[R-M-01]
[CONF]	ST31H320 B02 Configuration List, SMD_ST31H320_H_CFGL_B02, rev1.0	[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 EAL 2 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