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-2015/59-M01

ST31H320 A02 including optional cryptographic library NESLIB

Certificat de référence : ANSSI-CC-2015/59

Paris, le 20 avril 2016

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

Contre-amiral Dominique RIBAN
[ORIGINAL SIGNE]

1. Références

[CER]	Rapport de certification ANSSI-CC-2015/59 – ST31H320 A01 including optional cryptographic library NESLIB, du 28 décembre 2015, ANSSI.
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[IAR]	Security impact analysis report - ST31H320 Maskset K8N0A revision D (TOE rev A02) including optional lirabry Neslib, SMD_ST31H320-D_A02_SIA_15_001, version 1.2 du 26 janvier 2016, 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, juillet 2014.

2. Identification du produit maintenu

Le produit maintenu est le microcontrôleur sécurisé « *ST31H320 A02 including optional cryptographic libray NESLIB* » développé par *STMICROELECTRONICS*.

Le produit « *ST31H320 A01 including optional cryptographic library NESLIB* » a été certifié sous la référence ANSSI-CC-2015/59 (référence [CER]).

La version maintenue du produit est identifiable par l'élément suivant : *IC version* D.

Cette valeur est disponible 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 :

- des correctifs très ponctuels ont été effectués au niveau des masques de métal pour ajuster les caractéristiques électriques de l'I/O ;
- des clarifications (typographiques, éléments de caractérisation) et corrections non sécuritaires ont été apportées dans les guides utilisateurs [GUIDES].

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables, du produit évalué et sont 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.
Les guides contenant de nouvelles recommandations sécuritaires obligatoires par rapport au certificat initial apparaissent en gras, le cas échéant.

[GUIDES]	ST31H platform ST31H320, Datasheet – preliminary data, DS_ST31H320 Rev 2, janvier 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 2, novembre 2015, STMicroelectronics	[CER]
	ST31 firmware, User manual, UM_ST31_FW Rev 6, novembre 2015, STMicroelectronics	[R-M01]
	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	[R-M01]
	ST31H320 Flash memory loader installation guide, User manual, UM_31H_FL Rev 3, juillet 2015, 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_31_AIS31 Rev 2, février 2013, STMicroelectronics	[CER]
[ST]	Cible de sécurité de référence : - ST31H320 A02 including optional cryptographic library NESLIB, Security Target, SMD_ST31H320_ST_14_001 Rev A02.0, janvier 2016, STMicroelectronics. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée : - ST31H320 A02 including optional cryptographic library NESLIB, Security Target for composition, SMD_ST31H320_ST_14_002 Rev A02.0, janvier 2016, STMicroelectronics.	[R-M01] [R-M01]
[CONF]	Configuration list –ST31H320 Maskset K8N0A revision D (TOE rev A02) including optional library Neslib, SMD_ST31H320-D_A02_CFGL_001, 24 mars 2016, STMicroelectronics.	[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, à la date de certification.

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

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

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 :