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-2012/77-M04

Microcontroleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib 3.1

Certificat de référence : ANSSI-CC-2012/77

Paris, le 10 février 2017

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

Colonel Emmanuel GERMAIN
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2012/77 – Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib 3.1, 8 novembre 2012, ANSSI.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2012/77-S01, ST23R160B & produits dérivés, 4 décembre 2013, ANSSI
[R-S02]	Rapport de surveillance ANSSI-CC-2012/77-S02, ST23R160 & produits dérivés, 22 décembre 2014, ANSSI
[R-S03]	Rapport de surveillance ANSSI-CC-2012/77-S03, ST23R160 & produits dérivés, 25 août 2016, ANSSI
[MAI]	Procédure MAI/P/01 Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2012/77-M01, Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1, 11 juillet 2013, ANSSI.
[R-M02]	Rapport de maintenance ANSSI-CC-2012/77-M02, Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1, 4 mars 2014, ANSSI.
[R-M03]	Rapport de maintenance ANSSI-CC-2012/77-M03, Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib 3.1, du 19 février 2015.
[IAR]	Impact Analysis Report – Development Environment Evolution on ST23 Platform, SMD_ST23YR80&R160_SIA_16_001, v01.03, 23 novembre 2016, STMicroelectronics.
[RM-Lab]	Evaluation Technical Report Addendum Lafite Project, Lafite_ETR_ADD_v1.1, 25 janvier 2017, Serma Safety & Security.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 8th, 2010, Management Committee.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.

2. Identification du produit maintenu

Les produits maintenus sont les microcontrôleurs sécurisés ST23R160/R80A/R48A et ST23L160/ST23L80A/48A incluant optionnellement la bibliothèque cryptographique NesLib 3.1 en révision interne C (maskset BCA), D (maskset BDA), E (maskset CEA) ou F (maskset DFA) développés par la société *STMICROELECTRONICS*.

Les produits ont été initialement certifiés sous la référence ANSSI-CC-2012/77 (référence [CER]).

Ils ont déjà fait l'objet de trois maintenances sous les références ANSSI-CC-2012/77-M01 (voir [R-M01]), ANSSI-CC-2012/77-M02 (voir [R-M02]) et ANSSI-CC-2012/77-M03 (voir [R-M03]).

3. Description des évolutions

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

- Suppression d'un site de production Back End DISCO :
  - Disco HI-TEC Europe GmbH, Liebigstrasse 8, D-85551 Kirchheim beu Munchen, Germany.

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, 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-M04] référence la présente maintenance.

[GUIDES]	ST23L160, ST23L80A, ST23L48A, ST23R160, ST23R80A, ST23R48A – Enhanced security secure MCU with AES accelerator, up to 160 Kbyte EEPROM and dual or contact-only interface – Datasheet – DS_23R160 Rev 2.	[R-M02]
	ST23Rxxx Recommendations for contactless operations – Application note, AN_23R160_RCMD_CL Rev 2.	[R-M02]
	ST23 platform security guidance Application note, AN_SECU_23 Rev 12.	[R-S03]
	ST23Rxxx/ST23Lxxx Security guidance Application note, AN_23R160_SECU Rev2.	[CER]
	ST23 Secure MCU with AES NesLib Security Guidance – Application note, AN_23_AES_NesLib Rev 3.	[R-S02]
	How to identify certified hardware devices using additional ST traceability information (composite certification), AN_TRACE Rev 2.	[R-S01]
	NesLib 3.1 cryptographic library User Manual, UM_23_NesLib_3.1 Rev 5.	[R-S01]
	ST23 AIS31 compliant random numbers User Manual, UM_23_AIS31 Rev2.	[CER]
	ST23 AIS31 Reference implementation Start-up, Online and Total Failure Tests, AN_23_AIS31 Rev2..	[CER]
	ST21/23 programming manual, PM_21_23 Rev3.	[CER]
[ST]	ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A all with optional cryptographic library Neslib3.1, Security Target public version, SMD_ST23RLxxx_ST_11_001 Rev 04.01, Septembre 2016, STMicroelectronics.	[R-M04]
[CONF]	Addendum à la liste de configuration : Impact Analysis Report – Development Environment Evolution on ST23 Platform, SMD_ST23YR80&R160_SIA_16_001, Rev 01.03, 23 novembre 2016, STMicroelectronics.	[R-M04]

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 composants d'assurance du niveau CC EAL4 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, 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, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.