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-M03

Microcontroleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1

Certificat de référence : ANSSI-CC-2012/77

Paris, le 19 février 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

a) [MAI] Procédure MAI/P/01/2 Continuité de l'assurance
b) [ST] ST23R160/80A/48A *and* ST23L160/80A/48A Security Target, reference : SMD_Sx23xxxx_ST_10_001, v05.00, du 16 Janvier 2015, STMicroelectronics;
c) [ST Lite] *ST23R160/80A/48A and ST23L160/80A/48A Security Target Public Version*, référence : SMD_Sx23xxxx_ST_11_001, v04.00, du 16 Janvier 2015, STMicroelectronics;
d) [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, du 8 novembre 2012, ANSSI;
e) [M01] Rapport de maintenance ANSSI-CC-2012/77-M01, Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib 3.1, du 11 juillet 2013, ANSSI ;
f) [M02] Rapport de maintenance ANSSI-CC-2012/77-M02, Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib 3.1, du 4 mars 2014, ANSSI ;
g) [SUR] Rapport de surveillance ANSSI-CC-2012/77-S02 – ST23R160 & produits dérivés du 22 décembre 2014 ;
h) [IAR] Rapport d'analyse d'impact sécuritaire des produits ST23R160/80A/48A *and* ST23L160/80A/48A Maskset K2V0A internal rev D (contact) et C/E/F (RF), référence : SMD_ST23L160D-R160CEF_SIA_15_001, version 1.1 du 15 janvier 2015, STMicroelectronics;
i) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee ;
j) [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 ST23R160/80A/48A et ST23L160/80A/48A incluant optionnellement la bibliothèque cryptographique NesLib v3.1 en révision interne C (*maskset* BCA), D (*maskset* BDA), E (maskset CEA) ou F (maskset DFA) développés par STMicroelectronics.

Les produits ST23R160/80A/48A et ST23L160/80A/48A ont été initialement certifiés sous la référence ANSSI-CC-2012/77 en révision externe B et révision interne B (*maskset* BBA) (référence d).

Ces produits ont déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2012/77-M01 (référence e) et ANSSI-CC-2012/77-M02 (référence f).

Les produits objets de la présente maintenance sont les microcontrôleurs sécurisés :

- ST23R160/80A/48A (circuit en configuration « dual mode ») : révision externe B, révision interne C (maskset BCA) ;
- ST23R160/80A/48A (circuit en configuration « dual mode ») : révision externe C, révision interne E (maskset CEA) ;
- ST23R160/80A/48A (circuit en configuration « dual mode ») : révision externe D, révision interne F (maskset DFA) ;

- ST23L160/80A/48A (circuit en configuration « contact mode only ») : révision externe B, révision interne D (maskset BDA).

La révision interne des versions maintenues est identifiable par un octet en adresse C011h de la zone OTP de la mémoire EEPROM :

- « 43h » pour les unités de la révision interne C ;
- « 44h » pour les unités de la révision interne D ;
- « 45h » pour les unités de la révision interne E ;
- « 46h » pour les unités de la révision interne F.

3. Description des évolutions

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

- Pour ce qui concerne l'implémentation des produits : modifications de la rétro-modulation RF (ajustement de résistances). Cette évolution technique affecte uniquement les produits « R160/8A/48A » en révision F ; elle optimise leur performance RF, sans impact sur aucun élément sécuritaire. Les produits « L160/80A/48A » ne sont pas concernés.
- Pour ce qui concerne le cycle de vie : ajout d'un site audité dans le périmètre de l'environnement de développement des produits. Cela concerne les produits « R160/80A/48A » et « L160/80A/48A ».
    - STMicroelectronics, 850 rue Jean Monet, 38926 Crolles, France.

4. Fournitures prises en compte

Suite à la surveillance de ce produit (référence g) les guides ont été mis à jour. Les guides d'utilisation du produit sont désormais constitués des documents suivants :

[GUIDES]	Addendum aux guides identifiés dans le rapport de certification [CER] : – How to identify certified hardware devices using additional ST traceability information (composite certification), AN_TRACE Rev 2 ; – NesLib 3.1 cryptographic library User Manual, UM_23_NesLib_3.1 Rev 5 ; – ST23 platform security guidance Application note, AN_SECU_23 Rev 11 ; – ST23 Secure MCU with AES NesLib Security Guidance – Application note, AN_23_AES_NesLib Rev 3.

5. Fournitures impactées

Relativement à cette maintenance, les fournitures suivantes ont été mises à jour depuis le certificat initial :

[CONF]	Addendum à la liste de configuration : Security Impact Analysis Report – ST23L160/80A/48A – R160/80A/48A Maskset K2V0A internal rev D (contact) and C/E/F (RF) with optional Neslib 3.1, SMD_ST23L160D-R160CEF_SIA_15_001, v 1.1, 15 janvier 2015.
[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 – production data*, référence DS_23R160, révision 2 du 21 octobre 2013, STMicroelectronics.
	Application note : ST23Rxxx, recommendations for contactless operations, référence AN_23R160_RCMD_CL, révision 2 du 17 octobre 2013, STMicroelectronics.
[ST]	*ST23R160/80A/48A and ST23L160/80A/48A Security Target*, référence : SMD_Sx23xxxx_ST_10_001, v05.00, du 16 Janvier 2015.
	ST23R160/80A/48A and ST23L160/80A/48A Security Target - Public, référence : SMD_Sx23xxxx_ST_10_001, v04.00, du 16 Janvier 2015.

6. 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.

7. 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 ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

8. 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 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, Singapour, la Suède et la Turquie.