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-M02

Microcontrôleurs 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 4 mars 2014

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

[Original signé]

Contre-amiral Dominique RIBAN

SÉCURITÉ CERTIFICATION

1. Références

a) [MAI] Procédure MAI/P/01 Continuité de l'assurance ;

b) [CER] Rapport de certification ANSSI-CC-2012/77 - Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant la bibliothèque cryptographique NesLib 3.1, du 8 novembre 2012, ANSSI ;

c) [M01] Rapport de maintenance ANSSI-CC-2012/77-M01 ; Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant la bibliothèque cryptographique NesLib 3.1, du 11 juillet 2013 ;

d) [IAR] Rapport d'analyse d'impact sécuritaire des produits ST23R160/80A/48A and ST23L160/80A/48A Maskset K2V0A (révisions internes D et C/E), référence : SMD_ST23L160D-R160E_SIA_14_001, version 1.2 du 12 février 2014, STMicroelectronics ;

e) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee ;

f) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.

2. Identification du produit maintenu

Les produits ST23R160/80A/48A et ST23L160/80A/48A ont été initialement certifiés ANSSI-CC-2012/77 en révision externe B et révision interne B (*maskset* BBA, cf. référence « b »).

Une première maintenance a couvert ces produits dans leur révision externe B, en révision interne C (*maskset* BCA : circuit en configuration « dual mode ») et D (*maskset* BDA : circuit en configuration « contact mode only ») (cf. référence « c »).

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

La révision interne des versions maintenues du produit 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.

3. Description des évolutions

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

- pour ce qui concerne l'implémentation des produits : modification de la rétro-modulation RF (ajustement de résistances). Cette évolution technique affecte uniquement les produits « R160/80A/48A » en révision interne E ; 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 de plusieurs sites audités dans le périmètre de l'environnement de développement des produits. Cela concerne les produits « R160/80A/48A » et « L160/80A/48A ».

Les sites additionnels sont les suivants :

ST Sophia : 635 route des lucioles, 06560 Valbonne, France	**ST Grenoble** : 12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex, France
ST Calamba : 9 Mountain Drive, LISP II, Brgy La mesa, Calamba, Philippines 4027	**ST Ang Mo Kio 6** : 18 Ang Mo Kio Industrial park 2, Singapore 569505
CMP George Charpak : 880 Avenue de Mimet, 13541 Gardanne, France	

4. Fournitures impactées

Suite à cette maintenance, les fournitures suivantes ont été mises à jour :

[CONF]	Addendum à la liste de configuration : *Rapport d'analyse d'impact sécuritaire des produits ST23R160/80A/48A and ST23L160/80A/48A Maskset K2V0A* (révisions internes D et C/E), référence : SMD_ST23L160D-R160E_SIA_14_001, version 1.2 du 12 février 2014, STMicroelectronics.
[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.
[CIBLE]	*ST23R160/80A/48A and ST23L160/80A/48A Security Target*, référence : SMD_Sx23xxxx_ST_10_001, v04.00, du 27 janvier 2014, STMicroelectronics.

	ST23R160/80A/48A and ST23L160/80A/48A Security Target – Public version, référence : SMD_Sx23RLxxxx_ST_11_001, v03.00, du 24 janvier 2014, STMicroelectronics.

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 ré-évaluation 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, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

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.