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-M01

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 11 juillet 2013

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

[Original signé]

Patrick Pailloux

1. Références

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

b) [ST] *ST23R160/80A/48A and ST23L160/80A/48A Security Target*, référence : SMD_Sx23xxxx_ST_10_001, v03.00, 17 avril 2013.

c) [ST-public] *ST23R160/80A/48A and ST23L160/80A/48A Security Target – Public version*, référence : SMD_Sx23RLxxxx_ST_11_001, v02.00, 17 avril 2013.

d) Rapport de certification « Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib 3.1 », référence ANSSI-CC-2012/77, 8 novembre 2012.

e) [IAR] « Rapport d'analyse d'impact sécuritaire des produits ST23R160/80A/48A and ST23L160/80A/48A Maskset K2V0A (révisions internes C et D) », référence : SMD_ST23R160C-L160D_SIA_13_001, version 1.0, 8 avril 2013.

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

g) [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 maintenus sont les microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, en révision externe B, en révisions internes C (*maskset* BCA) ou D (*maskset* BDA) incluant optionnellement la bibliothèque cryptographique NesLib v3.1, développés par STMicroelectronics.

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

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 la révision interne C ;
- « 44h » pour la révision interne D.

3. Description des évolutions

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

- deux corrections de défauts fonctionnels sans impact sur la sécurité ont été effectuées dans les niveaux métalliques supérieurs ;
- une évolution correspondant au court-circuit à la masse des contacts d'antenne pour les dérivés en mode contact seul.

4. Fournitures impactées

Suite 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* – ST23R160/48A/18A-L160/48A/18A Maskset K2V0A internal revC and revD with optional Neslib 3.1, ref: SMD_ST23R160C-L160D_SIA_13_001, v1, 8 Avril 2013.
[GUIDES]	*ST23 Platform - Security Guidance*, référence AN_SECU_23, révision 10, STMicroelectronics.
	User manual: ST23 MCUs, NesLib 3.1 cryptographic library, référence UM_23_NesLib_3.1, revision 3, STMicroelectronics.
[ST]	*ST23R160/80A/48A and ST23L160/80A/48A Security Target*, référence SMD_Sx23xxxx_ST_10_001, v03.00, 17 avril 2013, STMicroelectronics.
	ST23R160/80A/48A and ST23L160/80A/48A Security Target – Public version, référence SMD_Sx23RLxxxx_ST_11_001, v02.00, 17 avril 2013, STMicroelectronics.

Note : les mises à jour des guides ne sont pas liées aux évolutions du produit. Elles ont eues uniquement pour but de rendre le texte plus compréhensible (pas d'ajout ou de retrait de recommandations).

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.