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-2010/02-M02

Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Certificat de référence : 2010/02

Paris, le 8 juillet 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

Références

1) Procédure MAI/P/01 Continuité de l'assurance ;
2) *Sx23YRxxB Security Target*, référence : SMD_Sx23Yrxx_ST_09_001, v01.00, STMicroelectronics ;
3) *Sx23YRxxB Security Target - Public Version*, référence : SMD_Sx23YRxx_ST_09_002, v02.01, STMicroelectronics ;
4) Rapport de certification ANSSI-CC-2010/02 - Microcontrôleurs sécurisés SA/B23YR48/80B, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 en configuration SA ou SB, du 10 février 2010, ANSSI ;
5) Rapport de maintenance ANSSI-CC-2010/02-M01 des produits SA/B23YR48/80B, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 en configuration SA ou SB, du 19 mars 2010, ANSSI ;
6) Rapport d'analyse d'impact sécuritaire des produits ST-SA-SB23YR80-48B Maskset BGB (incluant la liste de configuration de la révision interne G), référence : SMD_ST23YR80B_SIA_10_001, Avril 2010, STMicroelectronics ;
7) Avis du CESTI sur le SIA et la mise à jour des guides : *Note on the Sx23YR80G following hardware changes*, référence : Sx23YR870G_NOTE_01_v2.0, 28 juin 2010, Serma Technologies.

Identification du produit maintenu

Les produits maintenus sont les microcontrôleurs sécurisés SA/B23YR48/80B, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 en configuration SA ou SB, en révision externe B et révision interne G (*maskset* BGB).

Les produits SA/B23YR48/80B, développés par STMicroelectronics, ont été initialement certifiés ANSSI-CC-2010/02 (cf. référence 4) en révision externe B et révision interne F (*maskset* BFB), puis maintenus ANSSI-CC-2010/02-M01 (cf. référence 5) pour la mise à jour d'un guide de sécurité. Pour rappel, la certification initiale 2010/02 est, quant à elle, issue d'une réévaluation de ces mêmes produits certifiés ANSSI-CC-2009/51 (avec Neslib 2.0) puis ANSSI-CC-2009/62 (avec Neslib 3.0) en révision externe A et révision interne E.

Description des évolutions

Le rapport d'analyse d'impact de sécurité (cf. référence 6) mentionne que deux modifications ont été opérées sur les produits certifiés SA/B23YR48/80B (révision interne F). Ces modifications locales, qui n'ont nullement impacté le routage en place, ont été apportées pour améliorer le produit de manière à résoudre deux problèmes de caractérisation liés au redémarrage de la mémoire EEPROM sous certaines conditions et au contexte d'un calcul de Montgomery du coprocesseur cryptographique Nescrypt.

Ces évolutions n'introduisent aucun impact sur la consommation, les temps d'opérations et la sécurité des produits certifiés. L'impact sur la sécurité a donc été jugé mineur par l'analyse de STMicroelectronics (cf. référence 6). Cette analyse a été vérifiée et approuvée par le CESTI en charge de l'évaluation initiale (cf. référence 7).

STMicroelectronics a souhaité par ailleurs mettre à jour les guides utilisateurs (cf. [GUIDES]) en apportant des clarifications pour permettre aux utilisateurs d'avoir une meilleure compréhension des produits. Ces modifications ont été revues par le CESTI qui a confirmé (cf. référence 7) que celles-ci n'avaient aucun impact sur la sécurité des produits de la famille ST23.

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[CONF]	Liste de configuration : – Liste de configuration du produit SB23YR80B (révision interne E) initialement certifié ANSSI-CC-2009/62, Référence : SMD_SB23YR80E-UBT_CFGL_09_001 rev 1.1, STMicroelectronics ; – Rapport d'analyse d'impact sécuritaire des produits ST-SA-SB23YR80-48B Maskset BFB (incluant la liste de configuration de la révision interne F), référence : SMD_ST23YR80B_SIA_9_001, Novembre 2009, STMicroelectronics ; – Eléments de configuration impactés par les modifications déclarées dans le document cité en référence 6, Référence : cf. référence 6.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - ST23YR80 Datasheet, Référence : DS_23YR80 Rev 2, STMicroelectronics ; - ST23YR48 Datasheet, Référence : DS_23YR48 Rev 1, STMicroelectronics ; - ST23 Platform - Security Guidance, Référence : AN_SECU_23 Rev 7, STMicroelectronics ; - ST21/23 programming manual Référence : PM_21_23 Rev 2, STMicroelectronics ; - ST23YR80/48: Recommendations for contactless operation, Référence : AN_23YR80_RCMD Rev 4, STMicroelectronics ; - ST23 AIS31 Compliant Random Number User Manual, Reference : UM_23_AIS31 Rev 2, STMicroelectronics ; - ST23 AIS31 Tests reference implementation user manual, Reference : AN_23_AIS31 Rev2, STMicroelectronics ;

	- Addendum 1 – ST23 Platform Security Guidance, Reference : AN_SECU_23_AD1 Rev 1, STMicroelectronics ; - User Manual of Neslib 3.0 library, Reference : UM_23_NESLIB_3.0 Rev 2, STMicroelectronics ; - User Manual of Neslib 2.0 library, Reference : UM_NesLib_2.0 Rev 4, STMicroelectronics.

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.
Le niveau de confiance envers le produit maintenu est donc identique à celui de la version certifiée, à la date de certification (cf. référence 4).

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.

Reconnaissance du certificat

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 :

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

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[1], 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 :

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 ».

[1] 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.