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-2009/38-M01

Microcontrôleur sécurisé SA23YL80C et SB23YL80C, incluant la librairie cryptographique NesLib v1.0, v2.0 ou v3.0, en configuration SA ou SB

Certificat de référence : ANSSI-CC-2009/38

Paris, le - 5 AVR. 2011

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

Patrick Pailloux

SÉCURITÉ CERTIFICATION

Références

a) Procédure MAI/P/01 Continuité de l'assurance ;
b) *SA23YL80/SB23YL18/SA23YL80/SB23YL80 Security Target*, Référence : SMD_Sx23YLxx_ST_09_001, v01.00, STMicroelectronics ;
c) *SA23YL80C/SB23YL80C Security Target - Public Version*, Référence : SMD_Sx23YL80_ST_10_001, v01.00, STMicroelectronics ;
d) Rapport de certification ANSSI-CC-2009/38 - Microcontrôleur sécurisé ST23YL80C incluant la bibliothèque cryptographique NesLib SA v1.0, du 22 Octobre 2009, ANSSI ;
e) Rapport d'analyse d'impact sécuritaire des produits ST/SA/SB23YL80C *maskset* CIA (incluant la liste de configuration de la révision interne I), référence : SMD_ST23YL80I_SIA_10_001, Aout 2010, STMicroelectronics ;
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.*

Identification du produit maintenu

Les produits maintenus sont les microcontrôleurs sécurisés SA23YL80C et SB23YL80C (révision externe C) en révision interne I (*maskset* CIA), développés par STMicroelectronics, initialement certifiés ANSSI-CC-2009/38 en révision externe C et révision interne H (*maskset* CHA).

Description des évolutions

Le rapport d'analyse d'impact de sécurité mentionne que des modifications ont été opérées sur les produits certifiés SA23YL80C et SB23YL80C (révision interne I). Ces modifications locales, sans impact sur le routage du produit, ont été apportées pour améliorer le comportement du produit en cas de redémarrage, pour corriger l'instabilité d'une alarme de sécurité ainsi que pour pallier à une défaillance majeure du coprocesseur Nescrypt.

En plus de ces modifications hardware, les versions v2.0 et v3.0 de la librairie cryptographique Neslib ont été évaluées sur les produits SA23YL80C et SB23YL80C. La cible de sécurité de ces 2 produits a été mise à jour pour tenir compte de ces nouvelles versions de librairies cryptographiques.

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

STMicroelectronics a souhaité par ailleurs mettre à jour les guides utilisateurs, d'une part pour apporter des clarifications permettant aux utilisateurs d'avoir une meilleure compréhension des produits, d'autre part pour introduire une recommandation de contre-mesure (cf. référence AN_SECU_23_AD2) suite à une attaque nouvelle décrite par le CESTI sur un autre produit de la famille ST23, mais applicable aux produits SA23YL80C et SB23YL80C. Ces modifications ont été revues par le CESTI, qui a confirmé que celles-ci n'avaient aucun impact sur la sécurité des produits de la famille ST23Y.

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[CONF]	Liste de configuration : - *ST23YL80 and SA23YL80 products* - Configuration list (révision interne H), Référence : SCP_ST23YL80_CFGL_08_001 V01.02, STMicroelectronics, - Rapport d'analyse d'impact sécuritaire des produits ST/SA/SB23YL80C *maskset* CIA (incluant la liste de configuration de la révision interne I), Référence : SMD_ST23YL80I_SIA_10_001, Aout 2010, STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - *ST23YL80 Datasheet,* Référence : DS_23YL80 Rev 0.11, STMicroelectronics ; - *ST23 Platform - Security Guidance,* Référence : AN_SECU_23 Rev 7, STMicroelectronics ; - *ST23 Platform - Security Guidance - Addendum 1,* Référence : AN_SECU_23_AD1 Rev 2, STMicroelectronics ; - *ST23 Platform - Security Guidance - Addendum 2,* Référence : AN_SECU_23_AD2 Rev 1.1, STMicroelectronics ; - *ST21/23 programming manual,* Référence : PM_21_23 Rev 2, STMicroelectronics ; - *ST23 AIS31 Compliant Random Number User Manual,* Réference : UM_23_AIS31 Rev 2, STMicroelectronics ; - *ST23 AIS31 Tests reference implementation user manual,* Réference : AN_23_AIS31 Rev2, STMicroelectronics ; - *User Manual of Neslib 3.0 library,* Réference : UM_23_NESLIB_3.0 Rev 2, STMicroelectronics ; - *User Manual of Neslib 2.0 library,* Réference : UM_NesLib_2.0 Rev 4, STMicroelectronics ; - *User Manual of Neslib 1.0 library,* Réference : UM_NesLib_SA Rev 4, STMicroelectronics.
[ST]	- *Sx23YLxx Security Target (complete)*

	Référence : SMD_Sx23YLxx_ST_09_001.v01.00, *June 2008,* STMicroelectronics ; - *SA23YL80C/SB23YL80C Security Target (public)* Référence : SMD_Sx23YL80_ST_10_001.v01.00, *June 2010,* STMicroelectronics.

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.

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.

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].

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

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 :

[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.