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-2010/08-M01

Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Certificat de référence : ANSSI-CC-2010/08

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) *Sx23ZLxxA Security Target*, référence : SMD_Sx23ZLxx_ST_09_001, v01.00, STMicroelectronics ;
c) *Sx23ZLxxA Security Target - Public Version*, référence : SMD_Sx23ZLxx_ST_09_002, v01.00, STMicroelectronics ;
d) Rapport de certification ANSSI-CC-2010/08 - Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0 en configuration SA ou SB, du 8 Mars 2010, ANSSI ;
e) Rapport d'analyse d'impact sécuritaire des produits ST/SA/SB23ZL48/34/18A *maskset* ADA (incluant la liste de configuration de la révision interne D), référence : SMD_ST23ZL48D_SIA_10_001, Aout 2010, STMicroelectronics ;
f) Avis du CESTI sur le SIA, Evaluation Technical Report Sx23Yxxx, Sx23Zxxx, référence : *LAFITE-changes_ETR_v1.0 / 1.0*, Serma Technologies ;
g) [SOG-IS] *: "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, 8 Janvier 2010, Management Committee ;*
h) [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 SA23ZL48/34/18A et SB23ZL48/34/18A (révision externe A) en révision interne D (*maskset* ADA), développés par STMicroelectronics, initialement certifiés ANSSI-CC-2010/08 en révision externe A et révision interne C (*maskset* ACA).

Description des évolutions

Le rapport d'analyse d'impact de sécurité mentionne que des modifications ont été opérées sur les produits certifiés SA23ZL48/34/18A et SB23ZL48/34/18A (révision interne D). Ces modifications locales, sans impact sur le routage du produit, ont été apportées pour améliorer le comportement du produit en cas de redémarrage, le comportement de l'EEPROM, ainsi que pour pallier à une différence mineure du coprocesseur Nescrypt.

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 (cf. [GUIDES]), 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_23Z_AD1) suite à une attaque nouvelle décrite par le CESTI sur un autre produit de la famille ST23, mais applicable aux produits SA23ZL48/34/18A et SB23ZL48/34/18A. 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 ST23Z.

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[CONF]	Liste de configuration : - Liste de configuration du produit ST/SA/SB23ZL48/34/18A (révision interne C), Référence : SMD_STSB23ZL48_CFGL_09_001 rev 2.0, STMicrolectronics ; - Rapport d'analyse d'impact sécuritaire des produits ST/SA/SB23ZL48/34/18A *maskset* ADA (incluant la liste de configuration de la révision interne D), Référence : SMD_ST23ZL48A_SIA_10_001, Aout 2010, STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - *ST23ZL48 Datasheet,* Référence : DS_23ZL48 Rev 0.5, STMicroelectronics ; - *ST23ZL34 Datasheet,* Référence : DS_23ZL34 Rev 0.3, STMicroelectronics ; - *ST23ZL18 Datasheet,* Référence : DS_23ZL18 Rev 0.3, STMicroelectronics ; - *ST23Z Platform – Security Guidance,* Référence : AN_SECU_23Z Rev 2, STMicroelectronics ; - *ST23Z Platform - Security Guidance - Addendum 1,* Référence : AN_SECU_23Z_AD1 Rev 1, STMicroelectronics ; - *ST21/23 programming manual,* Référence : PM_21_23 Rev 2, STMicroelectronics ; - *Porting code from ST23Y to ST23Z devices,* Reference : AN_23_Porting 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.

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].
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'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.