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-2009/63-M01

Microcontrôleurs sécurisés SA23YL18B et SB23YL18B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Certificat de référence : ANSSI-CC-2009/63

Paris, le 21 MARS 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) *Sx23YLxx Security Target*, Référence : SMD_Sx23YLxx_ST_09_001, v01.00, STMicroelectronics ;
c) *SA23YL18B/SB23YL18B Security Target - Public Version*, Référence : SMD_Sx23YL18_ST_09_001, v01.00, Octobre 2009, STMicroelectronics ;
d) Rapport de certification ANSSI-CC-2009/63 - Microcontrôleurs sécurisés SA23YL18B et SB23L18B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, du 29 Avril 2010, ANSSI ;
e) Rapport d'analyse d'impact sécuritaire des produits ST/SA/SB23YL18B *maskset* BGA (incluant la liste de configuration de la révision interne G), référence : SMD_ST23YL18G_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 SA23YL18B et SB23YL18B (révision externe B) en révision interne G (*maskset* BGA), développés par STMicroelectronics, initialement certifiés ANSSI-CC-2009/63 en révision externe B et révision interne E (*maskset* BEA).

Description des évolutions

Le rapport d'analyse d'impact de sécurité mentionne que des modifications ont été opérées sur les produits certifiés SA23YL18B et SB23YL18B (révision interne G). 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 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, 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 SA23YL18B et SB23YL18B. 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.