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-2010/24-M01

Microcontrôleurs sécurisés SA23YT66/34A et SB23YT66/34A, incluant la librairie cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Certificat de référence : ANSSI-CC-2010/24

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) *SB/SA/ST23YT66/34 Security Target*, référence : SMD_Sx23YTxx_ST_09_001, v01.00, STMicroelectronics ;
c) *SB/SA23YT66A Security Target - Public Version*, référence : SMD_Sx23YTxx_ST_09_002, v01.00, STMicroelectronics ;
d) Rapport de certification ANSSI-CC-2010/24 - Microcontrôleurs sécurisés SA23YT66/34A et SB23YT66/34A, incluant la bibliothèque cryptographique NesLib v2.0 en configuration SA ou SB, du 11 mai 2010, ANSSI ;
e) Rapport d'analyse d'impact sécuritaire des produits ST/SA/SB23YT66/34A *maskset* AFB (incluant la liste de configuration de la révision interne F), référence : SMD_ST23YT66F_SIA_10_001, 4 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 SA23YT66/34A et SB23YT66/34A (révision externe A) en révision interne F (*maskset* AFB), développés par STMicroelectronics, initialement certifiés ANSSI-CC-2010/24 en révision externe A et révision interne C (*maskset* ACB).

Description des évolutions

Le rapport d'analyse d'impact de sécurité mentionne que des modifications ont été opérées sur les produits certifiés SA23YT66/34A et SB23YT66/34A (révision interne F). 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, pour pallier à une défaillance mineure du coprocesseur Nescrypt, ainsi que pour améliorer la tenue en ESD[1] du *Pad Xout*.

En plus de ces modifications hardware, la version v3.0 de la librairie cryptographique Neslib a été évaluée sur les produits SA23YT66/34A et SB23YT66/34A. Les cibles de sécurité de ces deux produits ont été mises à jour pour tenir compte de cette nouvelle version de librairie cryptographique.

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-

[1] *Electrostatic discharges*