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-2010/02-M03

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 : ANSSI-CC-2010/02

Paris, le 26 février 2013

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

a) [MAI] Procédure MAI/P/01 Continuité de l'assurance ;

b) *Sx23YRxxB Security Target - Public Version*, référence : SMD_Sx23YRxx_ST_09_002, v03.00, mars 2011, STMicroelectronics;

c) Rapport de certification ANSSI-CC-2010/02 - Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 10 février 2010, ANSSI ;

d) Rapport de Maintenance ANSSI-CC-2010/02-M01 - Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 19 mars 2010, ANSSI ;

e) 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, 8 juillet 2010, ANSSI ;

f) *Security Impact Analysis Report – ST-SA-SB23YR80- Maskset BHB or BIB with optional Neslib 2.0, 3.0 or 3.1 and with new FE and BE sites*, reference SMD_ST-SA-SB23YR80H-I_SIA_12_001, version 1.0, 3 décembre 2012, STMicroelectronics ;

g) Surveillance des produits Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, référence 2783/ANSSI/SDE/PSS/CCN, 27 septembre 2012, ANSSI ;

h) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee ;

i) [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 SA/SB23YR48B et SA/SB23YR80B, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 en configuration SA ou SB (révision externe B), en révision interne H (*maskset* BHB) et I (*maskset* BIB), développés par STMicroelectronics.

Les produits SA/SB23YR48B et SA/SB23YR80B, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 (révision externe B) en révision interne F (*maskset* BFB) ont été initialement certifiés ANSSI-CC-2010/02 (référence c). Ils ont déjà fait l'objet de deux maintenances sous les références ANSSI-CC-2010/02-M01 (référence d) et ANSSI-CC-2010/02-M02 (référence e) pour la révision externe B et révision interne G (*maskset* BGB).

Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence f) mentionne que les modifications suivantes ont été opérées :

- pour ce qui concerne le cycle de vie : ajout de plusieurs sites audités dans le périmètre de l'environnement de développement des produits ;
- pour ce qui concerne l'implémentation matérielle des produits :
  - pour la révision interne H : traitement d'un problème marginal de synchronisation d'horloge ;
  - pour la révision interne I : création d'une version contact seul des produits.

Les sites additionnels sont les suivants :

STMicroelectronics 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour	**ST Microelectronics** 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen P.R. Chine
STMicroelectronics 7 Loyang drive 508938 Singapour Singapour	**Smartflex Technologies** No 27, UBI rd 4, MSL building #04-04 408618 Singapour Singapour
DISCO Hi-Tec Europe GmbH Liebigstrasse 8 D-85551 Kirchheim bei Munchen Allemagne	**NEDCARD** Bijsterhuizen 25-29 6604 LM Wijchen Pay-Bas
GlobalFoundries (Singapore) 60 Woodlands industrial park D street 2 738406 Singapour Singapour	**STMicroelectronics (Morocco)** 101 Boulevard des Muriers 20 180 Bouskoura Maroc

Fournitures impactées

Fournitures prises en compte

Suite à la surveillance de ces produits (référence g) les guides ont été mis à jour. Les guides d'utilisation du produit sont désormais constitués des documents suivants :

[GUIDES]	- *ST23YR80 Datasheet*, référence DS_23YR80, révision 2.00, STMicroelectronics ; - *ST23YR48 Datasheet*, référence DS_23YR48, révision 1.00, STMicroelectronics ; - *ST23YR80/48 Recommendations for contactless operations*, référence AN_23YR80_RCMD, révision 4, STMicroelectronics ; - *ST23 Platform - Security Guidance*, référence AN_SECU_23, révision 10, STMicroelectronics ; - *Application note: ST23 secure MCUs with AES NesLib security guidance*, référence AN_23_AES_NesLib, révision 1, version 1, STMicroelectronics ; - *ST21/23 programming manual*, référence PM_21_23, révision 3, STMicroelectronics ; - *ST23 AIS31 Compliant Random Number User Manual*, référence UM_23_AIS31, révision 2, STMicroelectronics ; - *ST23 AIS31 Tests reference implementation user manual*, référence AN_23_AIS31, révision 2, STMicroelectronics ; - *User Manual of Neslib 2.0 library*, référence UM_23_NesLib_2.0, révision 5, STMicroelectronics ; - *User Manual of Neslib 3.0 library*, référence UM_23_NesLib_3.0, révision 3, STMicroelectronics.

Fournitures impactées

Suite à cette maintenance, les fournitures suivantes ont été également mises à jour depuis le certificat initial :

[CIBLE]	*SA23YR48B/SB23YR48B/SA23YR80B/SB23YR80B Security Target - Public Version*, référence SMD_Sx23YRxx_ST_09_002, version 03.00, mars 2011, STMicroelectronics.
[CONF]	Addendum à la liste de configuration : - *Security Impact Analysis Report – ST-SA-SB23YR80- Maskset BHB or BIB with optional Neslib 2.0, 3.0 or 3.1 and with new FE and BE sites*, reference SMD_ST-SA-SB23YR80H-I_SIA_12_001, version 1.0, 3 décembre 2012, 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 ré-évaluation 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 :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, 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 :

[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.