



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- M02

**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 26 février 2013

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

Patrick Pailloux
[ORIGINAL SIGNE]



Références

- a) [MAI] Procédure MAI/P/01 Continuité de l'assurance ;
- b) *Sx23ZLxxA Security Target*, référence SMD_Sx23ZLxx_ST_09_001, version 03.00, STMicroelectronics ;
- c) 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, 8 mars 2010, ANSSI ;
- d) 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, 5 Avril 2011, ANSSI ;
- e) *Security Impact Analysis Report – ST23ZL48/34/18A Maskset AGB*, reference SMD_ST23ZL48G_SIA_11_001, version 1.0, février 2012, STMicroelectronics ;
- f) Surveillance des produits Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, référence 2788/ANSSI/SDE/PSS/CCN, 27 septembre 2012, ANSSI ;
- 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 SA/SB23ZL48/34/18A, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 en configuration SA ou SB (révision externe A), en révision interne G (*maskset* AGB) développés par STMicroelectronics.

Les produits SA/SB23ZL48/34/18A, incluant la bibliothèque cryptographique Neslib 2.0 ou 3.0 (révision externe A) en révision interne C (*maskset* ACA) ont été initialement certifiés ANSSI-CC-2010/08 (référence c). Ils ont déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2010/08-M01 (référence d) pour la révision externe A et révision interne D (*maskset* ADA).

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 : ajustements matériels (*fixes*) ne modifiant aucune fonctionnalité de sécurité.

Les sites additionnels sont les suivants :

<p>STMicroelectronics</p> <p>629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour</p>	<p>ST Microelectronics</p> <p>16 Tao hua Rd. Futian free trade zone 518048 Shenzhen P.R. Chine</p>
<p>STMicroelectronics</p> <p>7 Loyang drive 508938 Singapour Singapour</p>	<p>Smartflex Technologies</p> <p>No 27, UBI rd 4, MSL building #04-04 408618 Singapour Singapour</p>
<p>STMicroelectronics (Morocco)</p> <p>101 Boulevard des Muriers 20 180 Bouskoura Maroc</p>	

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]	<ul style="list-style-type: none"> - <i>ST23ZL48 Datasheet</i>, référence DS_23ZL48, révision 3, STMicroelectronics ; - <i>ST23ZL34 Datasheet</i>, référence DS_23ZL34, révision 3 STMicroelectronics ; - <i>ST23ZL18 Datasheet</i>, référence DS_23ZL18, révision 3, STMicroelectronics ; - <i>ST23Z Platform - Security Guidance</i>, référence AN_SECU_23Z, révision 3, STMicroelectronics ; - <i>Application note: ST23 secure MCUs with AES NesLib security guidance</i>, référence AN_23_AES_NesLib, révision 1, version v1, STMicroelectronics ; - <i>ST21/23 programming manual</i>, référence : PM_21_23, révision 3, STMicroelectronics ; - <i>ST23 AIS31 Compliant Random Number User Manual</i>, reference UM_23_AIS31, révision 2, STMicroelectronics ; - <i>ST23 AIS31 Tests reference implementation user manual</i>, référence AN_23_AIS31, révision 2, STMicroelectronics ; - <i>User manual: ST23 MCUs, NesLib 3.0 cryptographic library</i>, référence UM_23_NesLib_3.0 Rev3, version 3,
----------	--

	<p>STMicroelectronics ;</p> <ul style="list-style-type: none">- <i>User manual: ST23 MCUs, NesLib 2.0 cryptographic library</i>, référence UM_23_NesLib_2.0 Rev4, version 4, STMicroelectronics.
--	--

Fournitures impactées

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

[CIBLE]	<p><i>SA-SB23ZL48A/SA-SB23ZL34A/SA-SB23ZL18A Security Target - Public Version</i>, référence : SMD_Sx23ZLxx_ST_09_002, v03.00 de décembre 2011, STMicroelectronics.</p>
[CONF]	<p>Addendum à la liste de configuration :</p> <ul style="list-style-type: none">- <i>Security Impact Analysis Report – ST23ZL48/34/18A Maskset AGB</i>, reference SMD_ST23ZL48G_SIA_11_001, version 1.0, février 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'accord¹, 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 signataires², 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'Autriche, 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.