



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-2010/07-M02

Microcontrôleurs sécurisés ST23ZL48A, ST23ZL34A et ST23ZL18A

Certificat de référence : ANSSI-CC-2010/07

Paris, le 17 octobre 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]



Références

- a) Procédure MAI/P/01 Continuité de l'assurance ;
- b) *Sx23ZLxxA Security Target*, référence SMD_Sx23ZLxx_ST_09_001, v01.00, STMicroelectronics ;
- c) *ST23ZLxxA Security Target - Public Version*, référence SMD_ST23ZLxx_ST_09_001, v03.00, décembre 2011, STMicroelectronics ;
- d) Rapport de certification ANSSI-CC-2010/07 - Microcontrôleurs sécurisés ST23ZL48/34/18A, 8 Mars 2010, ANSSI ;
- e) Rapport de Maintenance ANSSI-CC-2010/07-M01 - Microcontrôleurs sécurisés ST23ZL48/34/18A, 5 Avril 2011, ANSSI ;
- f) Rapport d'analyse d'impact sécuritaire des produits ST23ZL48/34/18A *maskset* ADA (incluant la liste de configuration de la révision interne D), référence SMD_ST23ZL48D_SIA_11_001, version 1.1, décembre 2011, STMicroelectronics ;
Rapport d'analyse d'impact sécuritaire des produits ST23ZL48/34/18A *maskset* AGB (incluant la liste de configuration de la révision interne G), référence SMD_ST23ZL48G_SIA_11_001, version 1.0, février 2012, STMicroelectronics ;
- g) Rapport de visites de sites de l'environnement de développement de STMicroelectronics, ST_VISIT_02_v1.1, janvier 2012, Serma Technologies ;
- h) Rapport de Surveillance du projet LAFITE, LAFITE-ST23Z_STR_v1.0, du 31 Mai 2011, SERMA TECHNOLOGIES;
- i) Project LAFITE (ST23ZLxx devices), Note on reported changes, LAFITE-changes_NOTE_04_v1.0 de mai 2012, Serma Technologies ;
- j) [SOG-IS] « *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates* », version 3.0, 8 janvier 2010, *Management Committee* ;
- k) [CC RA] *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, mai 2000.

Identification du produit maintenu

Les produits maintenus sont les microcontrôleurs sécurisés ST23ZL48A, ST23ZL34A et ST23ZL18A en révision externe A et révision interne G (*maskset* AGB) développés par STMicroelectronics.

Les produits ST23ZL48A, ST23ZL34A et ST23ZL18A en révision externe A et révision interne C (*maskset* ACA) développés par STMicroelectronics, ont été initialement certifiés ANSSI-CC-2010/07 (référence d). Ils ont déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2010/07-M01 (référence e) pour la révision externe A et révision interne D (*maskset* ADA).

Description des évolutions

Les rapports d'analyse d'impact de sécurité (référence f) mentionnent 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 : ajustements matériels (« *fixes* ») ne modifiant aucune fonctionnalité de sécurité.

Les sites additionnels sont les suivants :

- phases de fabrication et tests des *wafers* :

GlobalFoundries

60 Woodlands industrial park
D street 2
Singapore 738406

STMicroelectronics

629 Lorong 4/6 Toa Payoh
Singapore 319521

STMicroelectronics

7 Loyang drive
Singapore 508938

STMicroelectronics

16 Tao hua Rd
Futian free trade zone
Shenzhen
P. R. China 518048

- phase d'assemblage et tests des puces :

STMicroelectronics

101 boulevard des Muriers
BP97
20180 Maroc

Smartflex Technologies

No 27, UBI rd 4
MSL building #04-04
Singapore 408618

STMicroelectronics a par ailleurs mis à jour les guides utilisateurs [GUIDES] pour, d'une part, apporter des clarifications permettant aux utilisateurs d'avoir une meilleure compréhension des produits, et d'autre part, prendre en compte les dernières recommandations des activités de surveillance des circuits de la famille ST23Z (référence h).

Ces modifications n'ont pas d'incidence sur les mécanismes de sécurité, sur la consommation et sur les temps d'opération du produit certifié. L'impact sur la sécurité a donc été jugé « mineur ».

Fournitures impactées

Les fournitures suivantes ont été mises à jour :

[CIBLE]	Cible de Sécurité: <ul style="list-style-type: none">- <i>ST23ZL48A/ST23ZL34A/ST23ZL18A Security Target - Public Version</i>, référence SMD_ST23ZLxx_ST_09_001, v03.00, décembre 2011, STMicroelectronics.
[CONF]	Liste de configuration : <ul style="list-style-type: none">- Rapport d'analyse d'impact sécuritaire des produits ST23ZL48/34/18A <i>Maskset</i> AGB (incluant la liste de configuration de la révision interne G), référence SMD_ST23ZL48G_SIA_11_001, version 1.0 de février 2012, STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants: <ul style="list-style-type: none">- <i>ST23ZL48 Datasheet</i>, référence DS_23ZL48 Rev 3, STMicroelectronics ;- <i>ST23ZL34 Datasheet</i>, référence: DS_23ZL34 Rev 3, STMicroelectronics ;- <i>ST23ZL18 Datasheet</i>, référence: DS_23ZL18 Rev 3, STMicroelectronics ;- <i>ST23Z Platform - Security Guidance</i>, référence: AN_SECU_23Z Rev 3, STMicroelectronics ;- <i>ST21/23 programming manual</i>, référence: PM_21_23 Rev 3, STMicroelectronics;- <i>ST23 AIS31 Compliant Random Number User Manual</i>, référence: UM_23_AIS31 Rev 2, STMicroelectronics ;- <i>ST23 AIS31 Tests reference implementation user manual</i>, référence: AN_23_AIS31 Rev2, STMicroelectronics.

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.

Le niveau de confiance envers le produit maintenu est donc identique à celui de la version certifiée, à la date de certification (référence d).

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 CCRA [CCRA].

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'Espagne, la Finlande, la France, 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.