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-2014/20-M01

Microcontrôleurs SAMSUNG S3FT9MF/MT/MS Revision 1 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4

Certificat de référence : ANSSI-CC-2014/20

Paris, le 20 novembre 2014

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

a) Procédure MAI/P/01 Continuité de l'assurance.

b) Security Target of S3FT9MF/S3FT9MT/S3FT9MS 16-Bit RISC Microcontroller for Smart Cards, référence: ST Klallam5 v1.4, version 1.4, Samsung.

c) Rapport de certification Microcontrôleurs SAMSUNG S3FT9MF/MT/MS Revision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4, 17 mars 2014, ANSSI-CC-2014/20.

d) Impact Analysis Report - S3FT9MF/S3FT9MT/S3FT9MS Revision Comparison (rev 0 vs rev 1), version 1.1, 25 mars 2014; Additional information about S3FT9MF/S3FT9MT/S3FT9MS IAR v1.1, 2 mai 2014.

e) Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 Janvier 2010, SOG-IS Management Committee.

f) Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.

2. Identification du produit maintenu

Les produits maintenus sont les Microcontrôleurs SAMSUNG S3FT9MF/MT/MS Revision 1 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 développés par la société Samsung.

Les produits « Microcontrôleurs SAMSUNG S3FT9MF/MT/MS Revision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 » ont été initialement certifiés sous la référence ANSSI-CC-2014/20 (référence c).

La version maintenue du produit est identifiable par la lecture d'un octet à l'offset 0x40002A : 0x01 pour la révision 1.0.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence d) mentionne que les modifications suivantes ont été opérées : la différence entre la révision 0 et la révision 1 réside dans l'amélioration de la fonctionnalité sans-contact. Plus précisément, la modification de la couche métallique permet maintenant d'abaisser la tension afin de répondre à la faible puissance développée en mode sans-contact, et ainsi augmenter l'intensité du courant.

4. Fournitures impactées

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

[ST]	- *Security Target of Samsung S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller*, version 1.5, référence : ST Klallam5 v1.5.pdf, 2 avril 2014, Samsung; - *Security Target lite of Samsung S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller*, version 1.1, référence : ST Lite S3FT9MF_MT_MS v1.1.pdf, 2 avril 2014, Samsung.

5. 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.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

6. 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.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

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 :

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[2], 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.