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-2012/70-M01

Microcontrôleurs SAMSUNG S3CT9KW, S3CT9KC et S3CT9K9 Revision 3.0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.2

Certificat de référence : ANSSI-CC-2012/70

Paris, le 22 octobre 2012

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

[ORIGINAL SIGNE]

Patrick PAILLOUX

SÉCURITÉ CERTIFICATION

Références

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

b) [ST] « KICKAPOO Security Target » v2.1, 30 Juillet 2012.

c) [ST-Lite] « KICKAPOO Security Target Lite » v2.2, 26 septembre 2012.

d) [CER] Rapport de certification ANSSI-CC-2012/70, « Microcontrôleurs SAMSUNG S3CT9KW, S3CT9KC et S3CT9K9 Revision 2.0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.2 », 10 octobre 2012.

e) [IAR] « Impact Analysis Report S3CT9KW/KC/K9 Revision Comparison between Revision 1, 2 and Revision 3 » v3.1, 10 Mai 2012.

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

g) [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 SAMSUNG S3CT9KW, S3CT9KC et S3CT9K9 Revision 3.0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.2 » développés par SAMSUNG.

Le paragraphe 2.2.2.2 du document [CONF] précise que le numéro de version de la puce est indiqué en EEPROM à l'adresse 0x50002A. Il correspond au numéro de la version en décimal précédé d'un zéro si le numéro ne comporte qu'un chiffre. Pour les produits considérés la valeur du numéro de version lue en EEPROM est « 03 ».

Description des évolutions

Une modification fonctionnelle mineure, sans impact sur la sécurité, a été apportée au niveau de l'interface de communication sans contact afin de minimiser les variations du procédé de fabrication sur la génération de courant dues à la technologie CMOS.
Comme mentionné au paragraphe 4.4 du document [CONF], seule la zone analogique a été modifiée.

Fournitures impactées

Seuls les documents suivants relatifs à l'identification du produit ont changé :

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3CT9KW/ S3CT9KC/ S3CT9K9*, référence: ST_v3.3, version 3.3, Samsung. - *Security Target Lite of Samsung S3CT9KW/ S3CT9KC/ S3CT9K9*, référence: ST_Lite_v3.2, version 3.2, Samsung.
[CONF]	Liste de configuration du produit : - *Project <KICKAPOO> Life Cycle Definition (Class ALC_CMC.4/ALC_CMS.5)*, référence: ALC_CMC_CMS_v3.6, version 3.6, Samsung.

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.
Le niveau de confiance dans cette révision 3.0 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 réévaluation 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 :

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.