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-2012/27-M01

SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 1

Certificat de référence : ANSSI-CC-2012/27

Paris, le 1er octobre 2012

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) [ST_Rev0] *Security Target of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, version 1.9,* 30 novembre 2011, Samsung Electronics Co, Ltd ;
c) [ST-lite_Rev0] *Security Target Lite of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, version 1.0,* 19 décembre 2011, Samsung Electronics Co, Ltd ;
d) [CER] Rapport de certification ANSSI-CC-2012/27 – SAMSUNG S3FT9KF/S3FFT9KT/S3FT9KS, *revision* 0, 14 Juin 2012, Samsung Electronics Co, Ltd ;
e) [IAR] *Project Cahokia Impact Analysis Report S3FT9KF/S3FT9KT and S3FT9KS Revision comparison (Revision 0 vs Revision 1),* 5 août 2011, Samsung Electronics Co, Ltd ;
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 S3FT9KF/S3FT9KT/S3FT9KS, révision 1 développés par Samsung Electronics.
Les éléments d'identification peuvent être vérifiés conformément à [CER]. Seule l'information d'identification de la révision est modifiée ; il s'agit de la valeur 0x01 pour la révision 1, obtenue par lecture d'un octet à l'adresse 0x40002A.

Description des évolutions

Le rapport d'analyse d'impact de sécurité [IAR] mentionne que des modifications ont été opérées sur le *layout* du composant afin d'améliorer ses performances en mode sans contact. Ces modifications ont porté :

- sur le *FDT*[1] *timer* afin d'obtenir, à haute vitesse, un meilleur enchaînement dans la communication entre la carte et son lecteur ;
- *sur le SOF*[2] *timer* afin d'éviter des répétitions de messages nuisibles aux performances.

Fournitures impactées

[CONF]	Liste de configuration : - *Life cycle definition (Class ALC_CMC.4/CMS.5),* version 2.0, 14 juin 2012, Samsung Electronics Co, Ltd.
[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16- bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, version 2.0,* 15 juin 2012, Samsung Electronics Co, Ltd ;

[1] *Frame Delay Time.*
[2] *Start Of Frame.*

	- *Security Target Lite of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16- bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, version 2.0,* 19 décembre 2011, Samsung Electronics Co, Ltd.
[TESTS]	Rapport de tests - *Project CAHOKIA Test report (modification items between rev 0 and rev 1), S3FT9KF, S3FT9KT and S3FT9KS, version 1.0,* 10 septembre 2012, Samsung Electronics Co, Ltd.

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.