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-2014/75-M01

SAMSUNG S3FV9QM/S3FV9QK, révision 5,

rev5_SW10_26_11_30_GU136_12_111_13_01_127 et
rev5_SW10_26_12_30_GU136_12_111_13_01_127

Certificat de référence : ANSSI-CC-2014/75

Paris, le 22 décembre 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) Cible de sécurité : Project Cayuse R2, Security Target of Samsung S3FV9QM/S3FV9QK, 29 mai 2014, référence ST Cayuse R2 v4.1, version 4.1.
c) Cible de sécurité publique : Security Target Lite of Samsung S3FV9QM/S3FV9QK, 29 mai 2014, référence ST Lite v4.0, version 4.0.
d) Rapport de certification ANSSI-CC-2014/75 émis le 6 novembre 2014.
e) Rapport d'analyse d'impact : Project < Cayuse R2 > Impact Analysis Report – S3FV9QM and S3FV9QK Revision Comparison (IC Revision 3 vs Revision 4 and Bootloader v2.5 vs v2.6), 28 novembre 2014, référence Cayuse_Rev4_IAR_v2.3, version 2.3.
f) Rapport d'analyse d'impact : Project < Cayuse R2 > Impact Analysis Report – S3FV9QM and S3FV9QK Revision Comparison (IC Revision 4 vs Revision 5), 8 décembre 2014, référence Cayuse_Rev5_IAR_v3.1, version 3.1.
g) Rapport technique d'évaluation : Evaluation Technical Report (ALC ETR) CAYUSE-R CAYUSE-R2 CAYUSE-2 CAYUSE2-R COWICHAN2, 10 décembre 2014, référence LETI.CESTI.SAM.ALC.001-v1.0.
h) [SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
i) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, juillet 2014.

2. Identification du produit maintenu

Le produit maintenu est le microcontrôleur « **SAMSUNG S3FV9QM/S3FV9QK** », révision 5, référence rev5_SW10_26_11_30_GU136_12_111_13_01_127 et rev5_SW10_26_12_30_GU136_12_111_13_01_127, développé par la société Samsung.

Le produit « SAMSUNG S3FV9QM/S3FV9QK » (révision 3, référence rev3_SW10_25_11_30_GU136_12_111_13_01_124 et rev3_SW10_25_12_30_GU136_12_111_13_01_124) a été initialement certifié sous la référence ANSSI-CC-2014/75 (référence d).

La version maintenue du produit est identifiable par les éléments suivants :

- microcontrôleur : **SAMSUNG S3FV9QM/S3FV9QK, révision 5** ;
- librairies logicielles : *Boot loader v2.6*, *Crypto Library v1.1* ou *v1.2* (optionnelle).

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire FLASH (non effaçable) :

- identification des microcontrôleurs par lecture de deux octets à l'adresse 0x400004 : 0x1A16 pour S3FV9QM ou 0x1A14 pour S3FV9QK ;
- version de l'IC : **0x05 (**pour la révision 5) par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :
    - *test ROM code* : 0x10 pour la révision 1.0 par lecture d'un octet à l'adresse 0x40002B ;
    - *bootloader code* : **0x26** pour la révision 2.6 par lecture d'un octet à l'adresse 0x400030 ;
    - *crypto library* : 0x011A pour la révision 1.1 (support pour les calculs cryptographiques RSA) ou 0x012A pour la révision 1.2 (support pour les

calculs cryptographiques RSA et ECC) par lecture de deux octets à l'adresse 0x40002C ;

- *DTRNG* (*Digital True Random Number Generator*) *library* : 0x03 pour la révision 3.0 par lecture d'un octet à l'adresse 0x40002F.

3. Description des évolutions

Les rapports d'analyse d'impact de sécurité (références e et f) mentionnent que les modifications suivantes ont été opérées :

- nouvelle révision de l'IC, révision 5, du fait de l'amélioration de la fonction de régulateur de tension ;
- nouvelle version du *bootloader*, version 2.6, du fait de la suppression d'instructions propriétaires qui faisaient partie de la TOE mais non des TSF ;
- mise à jour d'un guide (référence [GUIDE]), correction d'erreurs ;
- remplacement du site de programme de test **Giheung Plant / SR2 Building** et du site de conception du circuit **Giheung Plant/ SR3 Building** par :

  Hwasung Plant/ DSR Building
  1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do,
  Korea ;
- ajout d'une nouvelle ligne de fabrication au site de fabrication des wafers Giheung : **Giheung Plant/, Line 6, S1** ;
- remplacement du nom du site de stockage, sciage et de polissage des wafers ChangFeng Plant par **Inesa Plant**.

Le CESTI en charge de l'évaluation initiale a émis un rapport partiel d'évaluation (référence g) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

4. Fournitures impactées

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

[CONF]	Liste de configuration du produit : Life Cycle Definition (Class ALC_CMC.4/CMS.5), référence Cayuse_R2_ALC_CMC_CMS_V4.1, version 4.1, 18 septembre 2014, Samsung Electronics Co, Ltd.
[GUIDE]	Boot Loader Specification for S3FV9QM, 6 septembre 2014, référence S3FV9QM_QK_BootloaderSpecification_v1.2.7, version 1.2.7.
[ST]	Cible de sécurité de produit maintenu : - Project Cayuse R2, Security Target of Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, référence ST Cayuse R2 v5.0, version 5.0, 5 décembre 2014, Samsung Electronics Co, Ltd. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette maintenance : - Security Target Lite of Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA

	and ECC Library including specific IC Dedicated Software, référence ST Lite S3FV9QM_QK v5.0, version 5.0, 5 décembre 2014, Samsung Electronics Co, Ltd.

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.