PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de surveillance ANSSI-CC-2020/06-S01

S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated software

Reference : S3FT9MF_20201219, Revision 1 & 2

Certificat de référence : ANSSI-CC-2020/06

Paris, le 21 mai 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

AVERTISSEMENT

La surveillance du produit ne constitue pas en soi une recommandation d'utilisation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

1 Références

[CER]	S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated software certifié le 27 février 2020 sous la référence ANSSI-CC-2020/06.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[RS-Lab]	*Evaluation Technical Report (full ETR)* – KLALLAM5-R8 référence LETI.CESTI.KLA5R8.FULL.001 – V2.0 émis le 30/10/2020 par le centre d'évaluation CEA-LETI.
[ETR_COMP]	Pour le besoin des évaluations ou surveillances en composition avec ce produit le rapport technique pour la composition a été mis à jour : *Evaluation Technical Report (ETR for composition)* – KLALLAM5-R8 référence LETI.CESTI.KLA5R8.COMPO.001 – V2.0 émis le 30/10/2020 par le centre d'évaluation CEA-LETI.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation CEA LETI, permet d'attester que le produit « S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated software, Reference : S3FT9MF_20191219, Revision 1 & 2 », initialement certifié sous la référence [CER], peut être considéré comme résistant à des attaques de niveau AVA_VAN.5 dans les mêmes conditions et restrictions d'usage que celles définies dans [CER], complétées par les recommandations sécuritaires additionnelles intégrées au fil des surveillances successives dans [GUIDES].

Il est à noter que de nouvelles recommandations sécuritaires ont été ajoutées au titre de la présente surveillance. Si ces recommandations ne sont pas mises en œuvre, le produit ne peut pas être considéré comme résistant à des attaques de niveau AVA_VAN.5.

Le rapport d'évaluation pour composition [ETR_COMP] a été mis à jour pour refléter les résultats de cette dernière surveillance.

3 Guides applicables

Le tableau ci-dessous liste les guides applicables du produit évalué. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du guide correspondant.

En particulier, [S01] référence la présente surveillance.

Les guides contenant de nouvelles recommandations sécuritaires par rapport au certificat initial apparaissent en gras.

[GUIDES]	S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, référence : S3FT9XX_DTRNG_FRO_AN_v1.16, version 1.16, 27 mai 2019, SAMSUNG.	[CER]
	S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, référence : S3FT9XX_EHP_DTRNG_FRO_AN_v2.21, revision 2.21, 26 novembre 2019, SAMSUNG.	[CER]
	S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, référence : S3FT9XX_EHP_DTRNG_FRO_AN_v1.61.pdf, version 1.61, 4 juillet 2019, SAMSUNG.	[CER]
	S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, référence : S3FT9XX_EHP_DTRNG_FRO_AN_v2.01.pdf, version 2.01, 26 novembre 2019, SAMSUNG.	[CER]
	S3FT9XX, 16-bit CMOS Microcontroller for Smart Card, User's Manual, référence : S3FT9XX_UM_REV1.33, révision 1.33, 20 mars 2017, SAMSUNG.	[CER]
	User's manual errata, référence : S3FT9XX_UM1.33_Errata_v0.3.pdf, version 0.30, mars 2020, SAMSUNG.	[S01]
	Security Application Note for S3FT9MD/MC,MF/MT/MS, MH/MV/MG, référence : SAN_S3FT9MD_MF_MH_v3.0 version 3.0, 21 août 2020, SAMSUNG.	[S01]
	CM1 RSA/ECC Library API Manual, référence : CM1 RSA ECC Library APIManual v2.04 , version 2.04, 05 octobre 2020, SAMSUNG.	**[S01]**
	S3FT9MF / T9MT / T9MS Chip Delivery Specification, référence : S3FT9MF_DV22 version 2.2, décembre 2017, SAMSUNG.	[CER]
	Bootloader User's Manual for S3FT9xx Family Products, référence : S3FT9xx_80nm_BootloaderSpecification_v2.4 version 2.4, 23 mars 2017, SAMSUNG.	[CER]
	SecuCalm CPU CORE, Architecture Reference, référence : secu_calm_AR14, version AR14, 3 mars 2011, SAMSUNG.	[CER]