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-2020/93-S01

S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software

(S3FT9MH_20200702)

Certificat de référence : ANSSI-CC-2020/93

Paris, le 27 décembre 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]	Rapport de certification ANSSI-CC-2020/93, S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, référence : S3FT9MH_20200702, 18/12/2020.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[RS-Lab]	*Evaluation Technical Report (full ETR) - KLALLAM7-R5,* référence *LETI.CESTI.KLA7R5.FULL.001 - V2.0, 23/08/2021,* 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) - KLALLAM7-R5*, référence LETI.CESTI.KLA7R5.COMPO.001 - V2.0, 23/08/2021, CEA LETI.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation CEA LETI, permet d'attester que le produit « S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, référence S3FT9MH_20200702 », 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].

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

Le rapport de surveillance [RS-Lab] permet également d'attester que le cycle de vie du produit est conforme aux composants de la classe ALC définis dans [CER].

La périodicité de la surveillance de ce produit est de 1 an.

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, [R-S01] référence la présente surveillance.

[GUIDES]	*S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note*, version 1.16, 27 mai 2019, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, version 2.21, 26 novembre 2019, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, version 1.61, 4 juillet 2019, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, version 2.01, 26 novembre 2019, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	RSA/ECC Library API Manual, version 2.06, 5 août 2020, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	RSA/ECC Library API Manual, version 3.02, 5 août 2020, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	RSA/ECC Library API Manual, version 4.00, 23 juillet 2020, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	S3FT9XX 16-bit CMOS Microcontroller for Smart Card, référence S3FT9XX_UM_REV1.33, version 1.33, 20 mars 2017, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	User's Manual Errata of S3FT9XX UM Rev1.33, version 0.30, mars 2020, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	Security Application Note for S3FT9MD/MC, MF/MR/MS, MH/MV/MG, version 3.0, 21 août 2020, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	S3FT9MH/MV/MG Chip Delivery Specification, référence S3FT9MH_DV22, révision 2.2, mars 2017, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	Bootloader User's Manual for S3FT9xx Family Products, version 2.4, 23 mars 2017, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	Architecture Reference: SecuPalm CPU Core, version AR14, 3 mars 2011, SAMSUNG ELECTRONICS CO. LTD.	[CER]
	Cryptographic Mechanisms For S3FT9MH, version 0.0, 19 juillet 2021.	[R-S01]