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-2021/02-S01

# Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software

**Référence : S3FV9QM_20210504**

**Certificat de référence : ANSSI-CC-2021/02**

Paris, le 28 septembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

# 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-2021/02, Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, Référence : S3FV9QM_20200504, 15/01/2021. |
| [SUR] | Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01. |
| [RS-Lab] | *Evaluation Technical Report (full ETR) - CAYUSE-R5*, référence : LETI.CESTI.CAYR5.FULL.001, version 2.0, 31/03/2021<br>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 :<br>Evaluation Technical Report (ETR for composition) - CAYUSE-R5, référence : LETI.CESTI.CAYR5.COMPO.001, version 2.0, 31/03/2021<br>LETI. |

# 2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation LETI, permet d'attester que le produit « Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, Référence : S3FV9QM_20210504 », 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.

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.

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

| | | |
|---|---|---|
| [GUIDES] | TORNADO-E RSA/ECC Library API Manual, version 1.441, 8 juillet 2020, SAMSUNG | [CER] |
| | **TORNADO-E RSA/ECC Library API Manual, version 1.48, 18 mars 2021, SAMSUNG** | **[R-S01]** |
| | S3FV9xx HW DTRNG and DTRNG library application note, version 1.6, 8 juillet 2020, SAMSUNG | [CER] |
| | S3FV9xx HW DTRNG and DTRNG library application note, version 2.1, 6 juillet 2020, SAMSUNG | [CER] |
| | S3FV9QM/QK 32-Bit CMOS Microcontroller for Smart Card, User's Manual, révision 1.11, 5 décembre 2013, SAMSUNG | [CER] |
| | S3FV9Qx Security Application Note, version 2.0, 1 juin 2018, SAMSUNG Electronics Co. Ltd | [CER] |
| | S3FV9QM/QK Chip Delivery Specification, revision 3.2, mai 2016, SAMSUNG | [CER] |