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 certification ANSSI-CC-2021/15

S3FT9PF/S3FT9PT/S3FT9PS

(S3FT9PF_20210329)

Paris, le 26 avril 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié 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

Référence du rapport de certification **ANSSI-CC-2021/15**
Nom du produit **S3FT9PF/S3FT9PT/S3FT9PS**
Référence/version du produit **S3FT9PF_20210329**
Conformité à un profil de protection ***Security IC Platform Protection Profile*** certifié BSI-PP-0035
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 5 augmenté** ALC_DVS.2, AVA_VAN.5
Développeur **SAMSUNG ELECTRONICS CO. LTD.** 17 Floor, B-Tower, 1-1, Samsungjeonja-ro Hwaseong-si, Gyeonggi-do, 445-330, Corée du Sud
Commanditaire **SAMSUNG ELECTRONICS CO. LTD.** 17 Floor, B-Tower, 1-1, Samsungjeonja-ro Hwaseong-si, Gyeonggi-do, 445-330, Corée du Sud
Centre d'évaluation **CEA - LETI** 17 avenue des martyrs, 38054 Grenoble Cedex 9, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2. **SOG-IS**

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est la famille de microcontrôleurs « S3FT9PF/S3FT9PT/S3FT9PS » de référence S3FT9PF_20210329, développée par SAMSUNG ELECTRONICS CO. LTD.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité est conforme au profil de protection [PP0035].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support à la cryptographie asymétrique (dont signature et génération de clefs) ;
- le support à la génération de nombres non prédictibles.

1.2.3 *Architecture*

Les microcontrôleurs S3FT9PF, S3FT9PT et S3FT9PS sont constitués des éléments suivants :

- une partie matérielle comprenant :
  - un processeur *SecuCalm RISC 16bit* ;
  - des mémoires :
    - 32 Ko de ROM ;
    - 8,5 Ko de RAM dont 2.5 Ko pour le crypto-processeur TORNADO 2Mx2 ;
    - respectivement 304, 264 et 232 Ko de FLASH pour les modèles S3FT9PF, S3FT9PT et S3FT9PS ;
  - des modules périphériques : protection de la mémoire (MPU), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, gestion des entrées/sorties en mode contact (UART ISO 7816), génération de nombres aléatoires – DTRNG, coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO 2MX2 ;

- une partie logicielle composée :
    - o des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
    - o d'une bibliothèque (optionnelle) pour le DTRNG ;
    - o d'une bibliothèque (optionnelle) de calcul arithmétique pour la cryptographie asymétrique *TORNADO 2MX2 Secure RSA/ECC/SHA library* ;
    - o d'un *Secure Boot Loader* (utilisant le coprocesseur AES) permettant le chargement sécurisé du code utilisateur.

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La procédure d'identification est décrite dans le guide « *Chip Delivery Specification* » (voir [GUIDES]). La version certifiée du produit est identifiable par les valeurs attendues telles que mentionnées dans la Table 1 de la cible de sécurité.

1.2.5 *Cycle de vie*

Le produit est développé sur les sites présentés à la section 1.2.4 de la cible de sécurité. Le cycle de vie s'inscrit dans le cycle de vie standard décrit dans [PP0035].

1.2.6 *Configuration évaluée*

Le certificat porte sur les microcontroleurs et les bibliothèques logicielles qu'ils peuvent embarquer, tels que définis au 1.2.3 du présent rapport. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.

Au regard du cycle de vie, le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de *wafer*, ou à l'issue de la phase 4 lorsque le produit est livré en boitiers (micro-modules, etc.).

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2 Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation de la précédente version du produit certifiée sous la référence [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de son émission, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus sont mentionnés dans le rapport technique d'évaluation [RTE]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI, à l'exception des mécanismes relatifs au chargement de code (mis en œuvre avant la phase 7 du cycle de vie). Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

2.4 Analyse du générateur d'aléas

Les produits embarquent un générateur d'aléas, appelé DTRNG FRO, qui a fait l'objet d'une analyse par le CESTI.

Cette analyse n'a pas permis de mettre en évidence de biais statistique. Comme énoncé dans le document [REF], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

Ce générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation. Le générateur atteint le niveau « P2– High » revendiqué dans la cible de sécurité.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « S3FT9PF/S3FT9PT/S3FT9PS » de version S3FT9PF_20210329 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit « S3FT9PF/S3FT9PT/S3FT9PS, S3FT9PF_20210329 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

3.3.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est 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 puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

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 EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	*Security architecture description*
	ADV_FSP	1	2	3	4	5	5	6	**5**	*Complete semi-formal functional specification with additional error information*
	ADV_IMP				1	1	2	2	**1**	*Implementation representation of the TSF*
	ADV_INT					2	3	3	**2**	*Well-structured internals*
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**4**	*Semiformal modular design*
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	*Operational user guidance*
	AGD_PRE	1	1	1	1	1	1	1	**1**	*Preparative procedures*
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**4**	*Production support, acceptance procedures and automation*
	ALC_CMS	1	2	3	4	5	5	5	**5**	*Development tools CM coverage*
	ALC_DEL		1	1	1	1	1	1	**1**	*Delivery procedures*
	ALC_DVS			1	1	1	2	2	**2**	*Sufficiency of security measures*
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	**1**	*Developer defined life-cycle model*
	ALC_TAT				1	2	3	3	**2**	*Compliance with implementation standards*
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	*Conformance claims*
	ASE_ECD	1	1	1	1	1	1	1	**1**	*Extended components definition*
	ASE_INT	1	1	1	1	1	1	1	**1**	*ST introduction*
	ASE_OBJ	1	2	2	2	2	2	2	**2**	*Security objectives*
	ASE_REQ	1	2	2	2	2	2	2	**2**	*Derived security requirements*
	ASE_SPD		1	1	1	1	1	1	**1**	*Security problem definition*
	ASE_TSS	1	1	1	1	1	1	1	**1**	*TOE summary specification*
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	*Analysis of coverage*
	ATE_DPT			1	2	3	3	4	**3**	*Testing: modular design*
	ATE_FUN		1	1	1	1	2	2	**1**	*Functional testing*
	ATE_IND	1	2	2	2	2	2	3	**2**	*Independent testing: sample*
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**5**	*Advanced methodical vulnerability analysis*

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3FT9PF/S3FT9PT/S3FT9PS*, version 8.3, 26 février 2021. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Lite of Samsung S3FT9PF/S3FT9PT/S3FT9PS*, version 7.0, 26 février 2021.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) – KLALLAM2-R5*, LETI.CESTI.KLA2R5.FULL.001, v1.0, 5 mars 2021. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report (ETR for composition) – KLALLAM2-R5*, LETI.CESTI.KLA2R5.COMPO.001, v1.0, 5 mars 2021.
[CONF]	Liste de configuration du produit : *Configuration Management, Klallam2R5_ALC_CMC_CMS* version 5.1, 4 mars 2021.
[GUIDES]	– *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note for DTRNG FRO Library v6.0*, v1.17, 8 février 2021 ; – *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note for DTRNG FRO Library v6.1*, v2.22, 8 février 2021 ; – *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note for DTRNG FRO Library v8.0*, v3.0, 8 février 2021 ; – *S3FT9XX 16 bit CMOS Microcontroller for Smart Card User's Manual*, version 1.33 , mars 2017 ; – *User's Manual Errata of S3FT9XX UM Rev1.33*, version 0.30 , mars 2020 ; – *Security Application Note for S3FT9FD/FC/FB, PF/PT/PS, PE, FA*, version 3.1, 26 février 2021 ; – *TORNADO-2Mx2 RSA/ECC Library API Manual* (TN_T2Mx2_RSAECC_APIManual_v2.70), version 2.70, 12 mars 2020 ; – *TORNADO-2Mx2 RSA/ECC Library API Manual* (TN _T2Mx2 _RSAECC_APIManual_v2.63), version 2.63, 13 mars 2020 ; – *TORNADO-2Mx2 RSA/ECC Library API Manual* (TN _T2Mx2 _RSAECC_APIManual_v2.41), version 2.41, 12 mars 2020 ; – *S3FT9PF / T9PT / T9PS Chip Delivery Specification*, version 1.4, mars 2018 ; – *Bootloader User's Manual for S3FT9xx Family Products*, version 2.4, 23 mars 2017 ; – *SecuCalm CPU CORE, architecture reference*, version AR14, 3 mars 2011.
[PP0035]	*Protection Profile, Security IC Platform Protection Profile*, version 1.0, juin 2007. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0035-2007.
[CER]	Rapport de certification ANSSI-CC-2020/27, Samsung S3FT9PF/ S3FT9PT/ S3FT9PS version S3FT9PF_20200329, 11 mai 2020.

ANNEXE C. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	*Mandatory Technical Document - The Application of CC to Integrated Circuits*, version 3.0, février 2009.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.1, juin 2020.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[AIS 31]	*Functionality classes and evaluation methodology for physical random number generator*, AIS31, version 1, 25 septembre 2001, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.