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 certification ANSSI-CC-2020/06

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)

Paris, le 27 février 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

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-2020/06

Nom du produit

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

Référence/version du produit

Reference : S3FT9MF_20191219, Revision 1 & 2

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0,
certifié BSI-CC-PP-0084-2014 le 19 février 2014

avec conformité aux packages

“Loader dedicated for usage in Secured Environment only”
“Loader dedicated for usage by authorized users only”

Critères d’évaluation et version

Critères Communs version 3.1 révision 5

Niveau d’évaluation

EAL 6 augmenté
ASE_TSS.2

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

SOG-IS

Ce certificat est reconnu au niveau EAL2.

Préface

La certification

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 national 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 matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 6
1.2.4. Identification du produit 7
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. TRAVAUX D'EVALUATION 10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 10
2.4. ANALYSE DU GENERATEUR D'ALEAS 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RESTRICTIONS D'USAGE 11
3.3. RECONNAISSANCE DU CERTIFICAT 11
3.3.1. Reconnaissance européenne (SOG-IS) 11
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 14

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 17

1. Le produit

1.1. Présentation du produit

Le produit évalué est « 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 » développé 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.

Cette cible de sécurité est strictement conforme au profil de protection [PP0084], avec :
- le package « *loader dedicated for usage in secured environment only* » ;
- le package « *loader dedicated for usage by authorized users only* ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par les produits 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 ou asymétriques ;
- le support à la génération de nombres non prédictibles.

1.2.3. Architecture

Les produits sont constitués des éléments suivants :
- une partie matérielle[1] comprenant :
  - un processeur SecuCalm RISC 16 bits ;
  - des mémoires :

[1] La version 1 et la version 2 de la partie matérielle présentent des différences dans la gestion de l'alimentation, la version 2 permettant une communication sans-contact lorsque le microcontrôleur est alimenté en contact.

  - 32 Ko de ROM ;
  - 6 Ko de RAM, plus 2.5Ko dédiés au coprocesseur arithmétique ;
  - 264, 232 et 212 Ko de FLASH respectivement pour les modèles S3FT9MF, S3FT9MT et S3FT9MS ;
- des modules de sécurité : protection de la mémoire (MPU), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- des modules fonctionnels : gestion des entrées / sorties en mode contact (UART ISO 7816), génération de nombres aléatoires – DTRNG (*Digital True Random Number Generator*[1]) et BPRNG (*Bilateral Pseudo-Random Number Generator*) à usage interne uniquement, coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO 2MX2,

- une partie logicielle composée :
  - des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
  - de bibliothèques pour la génération de nombres aléatoires *DTRNG FRO library*, version 6.0 ou 6.1 et *EHP DTRNG FRO library*, version 2.0 ou 2.2 ;
  - de la bibliothèque pour la cryptographie asymétrique *TORNADO 2Mx2 CM1 Secure RSA/ECC/ECC library* version 2.04 ; cette bibliothèque est optionnelle et peut être désactivée ou absente lors de la livraison du microcontrôleur ;
  - d'un *Secure Boot Loader*, version 5.0, 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 version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.2.2 « TOE Definition ».

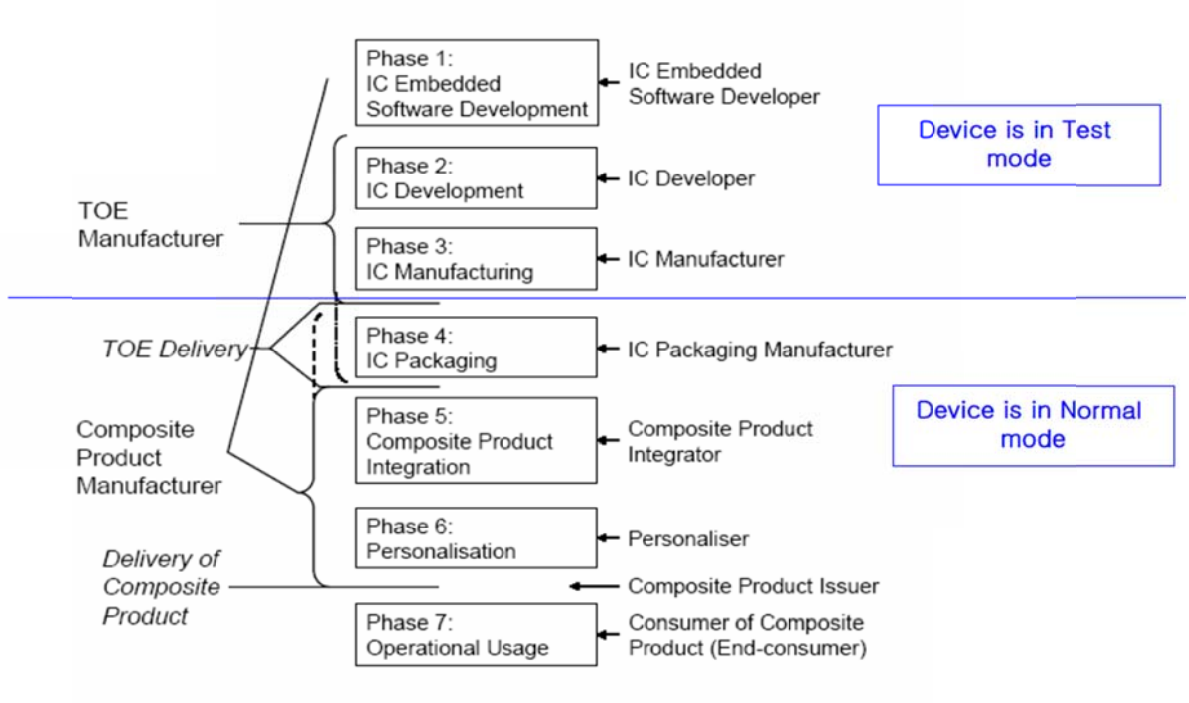
Eléments de configuration		Données d'identification lues
Identification des microcontrôleurs	*S3FT9MF*	0x160F
	S3FT9MT	0x161D
	S3FT9MS	0x161C
	Revision 1 ou Revision 2	0x01 ou 0x02
Identification des logiciels embarqués	*Test ROM Code version 1.0*	0x10
	Secure Boot loader version 5.0	0x50
Identification des bibliothèques	*CM1 Secure RSA/ECC/SHA Library version 2.04*	0x312E3034
	DTRNG FRO library version 6.0 ou version 6.1	0x0600 ou 0x0601
	EHP DTRNG FRO library version 2.2	0x0202

[1] Générateur physique de nombres aléatoires.

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide « S3FT9MF / T9MT / T9MS Chip Delivery Specification », voir [GUIDES].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants (voir [SITES]) :

Nom du Site	Adresse	Fonction
Hwasung Plant/ DSR Building	1, Samsungjeonja-ro, Hwasung-City, Gyeonggi-do, Corée du Sud	Phase 2 : *Smart Card Design Center*
Giheung Plant/ SR3 building	San #24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do, KOREA	Phase 3 : *Test program development*
Hwasung Plant/ NRD Building	San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 3 : *Mask Shop*
Giheung Plant/ Line 6, S1	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 446-711 Corée du Sud	Phase 3 : *Wafer Fabrication*
Giheung Plant/ Line 2		Phase 3 : *Inking / Giheung Wafer Stock*
Giheung Plant/ Line 1		Phase 3 : *Grinding*

Onyang Plant/ Warehouse	San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 4 : *Packing, Warehouse*
Onyang Plant/ Line 2		Phase 3&4 : *Stock, Grinding, Sawing, Packaging, Package Testing*
Onyang Plant/ Line 6		Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
PKL Plant	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : *External Mask Shop*
HANAMICRON plant	#95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
Inesa Plant	No. 818 Jin Yu Road Jin Qiao Export Processing Zone Pudong, Shanghai, Chine	Phase 3&4 : *Grinding, Sawing, COB*
		Phase 4 : *Packaging, Warehouse*
Eternal Plant	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 3&4 : *Sawing, COB*
		Phase 4 : *Packing, Warehouse*
TESNA Plant	450-2 Mogok-Dong, Pyeungtaek City, Gyeonggi, Corée du Sud	Phase 3 : Wafer *Testing, Pre-personalization*
ASE Korea	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, SIP module assembly*

1.2.6. Configuration évaluée

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au 1.2.3. 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 détaillé au chapitre 1.2.5, 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 boîtiers (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 du produit « S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated software, Revision 1 & 2 » certifié le 13 mai 2019 sous la référence ANSSI-CC-2019/22, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 février 2020, 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 selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Les produits embarquent un DTRNG, appelé DTRNG FRO, incluant un retraitement qui a fait l'objet d'une analyse par le CESTI. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception.

Le 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 level* ».

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 « 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 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 6 augmenté du ASE_TSS.2.

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 « 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 » 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.org.

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], 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 :

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

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance, EAL							Niveau d'assurance retenu pour le produit	
		1	2	3	4	5	6	7	6+	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	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**3**	Minimally complex internals
	ADV_SPM						**1**	1	**1**	Formal TOE security policy model
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**5**	Complete 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	**5**	Advanced support
	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	**3**	Compliance with implementation standards - all parts
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	**2**	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**3**	Rigorous analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**2**	Ordered 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 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, ST (Security Target), version 12.1, 28 novembre 2019, *SAMSUNG*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, ST (Security Target) Lite, version 12.0, 28 novembre 2019, *SAMSUNG*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – KLALLAM5-R8 - LETI.CESTI.KLA5R8.FULL.001, version 1.1, 21 février 2020, *CEA-LETI*. 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) – KLALLAM5-R8, LETI.CESTI.KLA5R8.COMPO.001, version 1.0, 3 décembre 2019, *CEA-LETI*.
[CONF]	Liste de configuration du produit : - Common Criteria Information Technology Security Evaluation – Klallam5 R8, référence : Klallam5R8_ALC_CMC_CMS_V12.0, version 12.0, 28 novembre 2019, *SAMSUNG*.

[GUIDES]	Guides du produit : - S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, référence : S3FT9XX_DTRNG_FRO_AN_v1.16, version 1.16, 27 mai 2019, *SAMSUNG* ; - 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* ; - 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* ; - 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* ; - S3FT9XX, 16-bit CMOS Microcontroller for Smart Card, User's Manual, référence : S3FT9XX_UM_REV1.33, révision 1.33, 20 mars 2017, *SAMSUNG* ; - User's manual errata, référence : S3FT9XX_UM1.33_Errata_v0.2.pdf, version 0.20, décembre 2018, *SAMSUNG* ; - Security Application Note for S3FT9MD/MC,MF/MT/MS, MH/MV/MG, référence : SAN_S3FT9MD_MF_MH_v2.9 version 2.9, 22 novembre 2019, *SAMSUNG* ; - CM1 RSA/ECC Library API Manual, référence : CM1 RSA ECC Library APIManual v2.03 , version 2.03, 27 novembre 2019, *SAMSUNG* ; - S3FT9MF / T9MT / T9MS Chip Delivery Specification, référence : S3FT9MF_DV22 version 2.2, décembre 2017, *SAMSUNG* ; - Bootloader User's Manual for S3FT9xx Family Products, référence : S3FT9xx_80nm_BootloaderSpecification_v2.4 version 2.4, 23 mars 2017, *SAMSUNG ;* - SecuCalm CPU CORE, Architecture Reference, référence : secu_calm_AR14, version AR14, 3 mars 2011, *SAMSUNG*.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

[CER]	« S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (Revision 1 & 2) ». *Certifié le 13 mai 2019 sous la référence ANSSI-CC-2019/22.*

Annexe 3. 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, version 2.9, janvier 2013.
[CC RA]	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]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, 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.