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-2020/12

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

Paris, le 3 mars 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

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-2020/12

Nom du produit

S3FT9MH/S3FT9MV/S3FT9MG

Référence/version du produit

S3FT9MH_20190702

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

“Authentication of the security IC”
“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 Premier ministre 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

1.1. Présentation du produit

Le produit évalué est la famille de microcontrôleurs « S3FT9MH/S3FT9MV/S3FT9MG » de référence S3FT9MH_20190702 développé par Samsung Electronics Co. Ltd. et Trusted Labs.

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 « *authentication of the security IC* » ;
- le package « *loader dedicated for usage in secured environment only* » ;
- le package « *loader dedicated for usage by authorized users only* ».

Comme clairement décrit dans la cible de sécurité, certaines variantes du produit ne revendiquent pas la conformité à l'ensemble de ces packages.

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 ou asymétriques ;
- le support à la génération de nombres aléatoires.

1.2.3. Architecture

Le produit est constitué :
- une partie matérielle comprenant :
  - un processeur SecuCalm RISC 16 bits ;
  - des mémoires, dont :
    - 40 Ko de ROM, partiellement occupés par les logiciels de test embarqués (*Test ROM Code*) ;
    - 9 Ko de RAM, ainsi que 5Ko de RAM dédiés au coprocesseur arithmétique ;

        - 500, 420 et 320 Ko de FLASH respectivement pour les modèles S3FT9MH, S3FT9MV et S3FT9MG ;
    - des modules de contrôle : 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 FRO et BPRNG (*Bilateral Pseudo-Random Number Generator*, à usage interne uniquement), coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques *TORNADO E* ;
- une partie logicielle composée :
    - des logiciels de test du microcontrôleur (*Test ROM code*, version 1.0) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
    - de bibliothèques pour la génération de nombres aléatoires *DTRNG FRO library*, en version 7.0 ou 7.1, et *EHP DTRNG FRO library*, en version 1.0 ou 2.1 ;
    - d'une bibliothèque pour la cryptographie asymétrique *Secure RSA/ECC/SHA library*, en version 2.04 ou 2.06, qui utilise l'accélérateur *TORNADO-E ;*
    - d'un logiciel *Secure Boot Loader*, en version 4.9 ou 5.0 selon la révision de l'IC (0 ou 1), 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, de référence S3FT9MH_20190702, diffère de la version précédente du produit, certifiée sous la référence ANSSI-CC-2018/33 (voir [CER]), en cela qu'elle ajoute une nouvelle version de la bibliothèque cryptographique et des bibliothèques de génération d'aléa à celles déjà présentes dans le précédent produit. La version certifiée est donc identifiable par les valeurs identifiant la version certifiée dans [CER] auxquelles s'ajoutent les valeurs correspondant aux nouvelles bibliothèques. Ces valeurs attendues sont donc les suivantes :

- identification des microcontrôleurs :
    - 0x1611, 0x161F ou 0x1610 désignant respectivement les modèles S3FT9MH, S3FT9MV et S3FT9MG ;
- Révision matérielle :
    - 0x00 ou 0x01 respectivement pour la révision 0 (avec *Secure Boot Loader* en version 4.9) et la révision 1 (*Secure Boot Loader* en version 5.0) ;
- identification des logiciels embarqués :
    - *Test ROM Code* : 0x10 pour la version 1.0 ;
    - *Secure Boot loader* : 0x49, 0x50 respectivement pour la version 4.9 (pour la révision 0 du microcontrôleur) et la version 5.0 (pour la révision 1 du microcontrôleur) ;
    - *Secure RSA/ECC/SHA library* : « PKA_Lib_CE1_v2.04 » ou « PKA_Lib_CE1_v2.06 » respectivement pour la version 2.04 et la version 2.06 ;
    - *DTRNG FRO Library* : 0x0700 ou 0x0701 respectivement pour la version 7.0 et la version 7.1 ;
    - *EHP DTRNG FRO Library Version* : 0x0100 ou 0x0201 respectivement pour la version 1.0 et la version 2.1.

1.2.5. Cycle de vie

Le cycle de vie du produit correspond à celui décrit dans le profil de protection ([PP0084]) et peut être représenté par le schéma suivant :

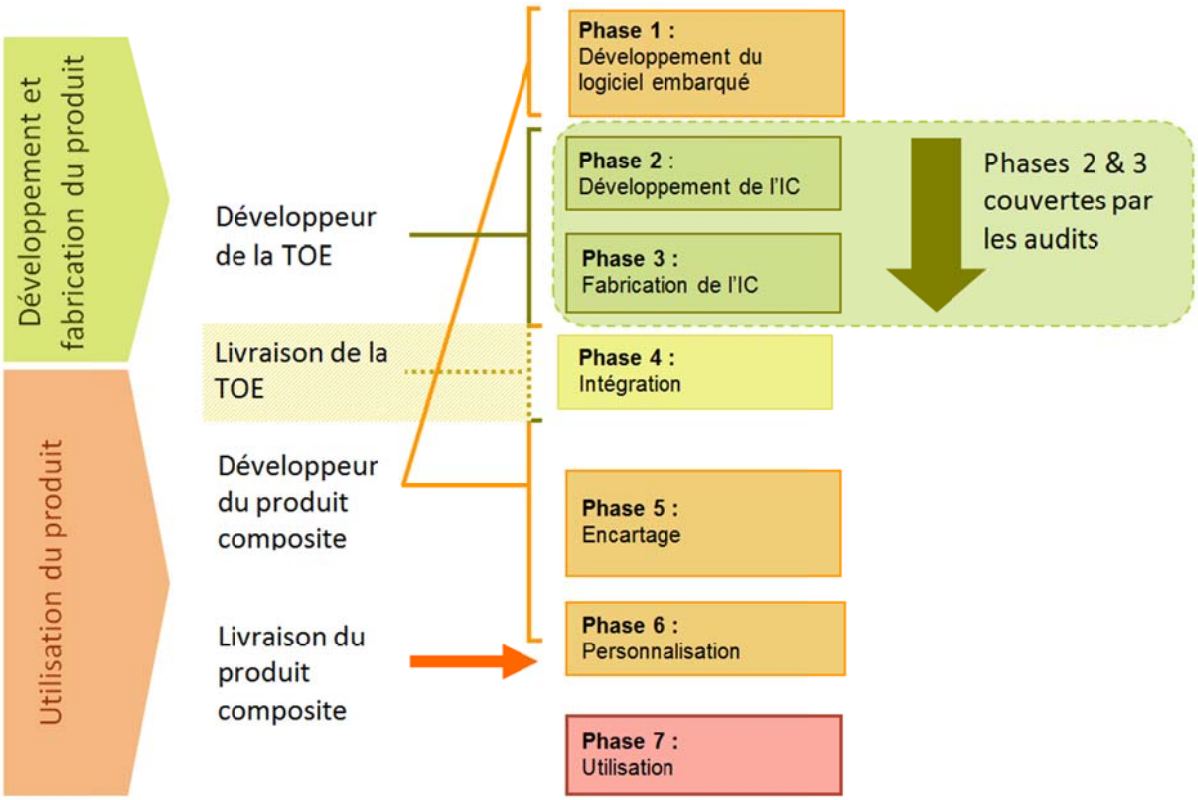

Figure 1 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de *wafers*. En option, la TOE peut également être livrée intégrée en boîtiers après la phase 4.

La phase 2 correspond à la phase de développement du microcontrôleur et comprend notamment les étapes suivantes :

- conception du circuit ;
- développement du logiciel dédié.

La phase 3, qui couvre la fabrication du microcontrôleur, comprend les étapes suivantes :

- intégration et fabrication du masque ;
- fabrication du circuit ;
- test du circuit ;
- préparation ;
- pré-personnalisation si nécessaire.

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

Hwasung Plant / DSR building	**Hwasung Plant / NRD building**
1, Samsungjeonja-ro (Banwol-Dong) Hwasung-City, Gyeonggi-Do Corée du Sud	San #16, Banwol-Dong Hwasung-City, Gyeonggi-Do Corée du Sud

Giheung Plant, lines 6 S1, 2 et 1 San #24, Nongseo-Dong, Giheung-Gu Tongin-City, Gyeonggi-Do Corée du Sud	**Onyang Plant / Warehouse, line 2 et line 6** 158 Baebang-ro Baebang-eup Asan-si Chungcheongnam-do Corée du Sud 31489
PKL Plant 493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	**HANA Micron Plant** 77 Yeonamyulgeum-ro, Umbong-Myeon, Asan-Si, Chung-Nam, Corée du Sud
Inesa Plant No. 818 Jin Yu Road Jin Qiao Export, Zone Pudong, Chine	**TESNA Plant** 450-2 Mogok-Dong, Pyeung-taek City, Gyeonggi, Corée du Sud
ASE Korea 76, Sanupdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	

1.2.6. Configuration évaluée

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils peuvent embarquer tels que définis au 1.2.2. 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 certifié le 22 août 2018 sous la référence ANSSI-CC-2018/33, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18 juillet 2019, 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 vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le produit embarque un générateur physique d'aléa appelé DTRNG FRO, qui a fait l'objet d'une analyse par le CESTI et par l'ANSSI. Ce générateur a fait l'objet d'une analyse.

Les règles RègleArchiGVA-1 et RègleArchiGVA-2 ainsi que la recommandation RecomArchiGVA-1 de [REF] s'avèrent respectées, lorsque DTRNG FRO est utilisé comme indiqué en §2.3.2 du guide « *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note* » (en version 1.16 et 2.2, voir [GUIDES]). Le document [REF] impose, pour un usage cryptographique, que la sortie d'un générateur matériel de nombres aléatoires subisse un retraitement algorithmique de nature cryptographique ; ce retraitement n'est pas implémenté dans le produit et devra être développé par l'utilisateur le cas échéant.

Le générateur d'aléa DTRNG FRO, utilisé comme indiqué en §2.3.3 du guide *« S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note »* (voir [GUIDES]), répond aux exigences de la classe PTG.2 de la méthodologie [AIS31].

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 « S3FT9MH/S3FT9MV/S3FT9MG », référence S3FT9MH_20190702, 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/des composant(s) 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 « S3FT9MH/S3FT9MV/S3FT9MG », référence S3FT9MH_20190702, 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 microcircuit 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.

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							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 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	**2**	1	**2**	TOE summary specification wit 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 1. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target of S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Library including specific IC Dedicated Software, référence ST_Klallam7R4_V6.3, version 6.3, daté du 10 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.*. 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 S3FT9MH/S3FT9MV/S3FT9MG, référence ST_Lite_S3FT9MH_MV_MG_V5.1, version 5.1, daté du 10 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical report (full ETR) – KLALLAM7-R4, référence LETI.CESTI.KLA7R4.FULL.001 – V1.1, version 1.1, daté du 18 juillet 2019, *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) – KLALLAM7-R4, référence LETI.CESTI.KLA7R4.COMPO.001 – V1.1, version 1.1, daté du 18 juillet 2019, *CEA-LETI.*
[CONF]	Liste de configuration du produit : - Klallam7R4 Life Cycle Definition (Class ALC_CMC.5/CMS.5), version 5.1, daté du 10 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.*.

[GUIDES]	Guides du produit : - S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, référence S3F9XX_DTRNG_FRO_AN_v1.16, version 1.16, daté du 27 mai 2019, *SAMSUNG ELECTRONICS CO. LTD.* ; - S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, référence S3F9XX_DTRNG_FRO_AN_v2.2, version 2.2, daté du 7 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.* ; - S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, référence S3F9XX_EHP_DTRNG_FRO_AN_v1.61, version 1.61, daté du 4 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.* ; - S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, référence S3F9XX_EHP_DTRNG_FRO_AN_v2.0, version 2.0, daté du 5 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.* ; - RSA/ECC Library API Manual, version 2.04, daté du 9 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.* ; - RSA/ECC Library API Manual, version 3.00, daté du 4 juillet 2019, *SAMSUNG ELECTRONICS CO. LTD.* ; - S3FT9XX 16-bit CMOS Microcontroller for Smart Card, référence S3FT9XX_UM_REV1.33, version 1.33, daté du 20 mars 2017 ; - Security Application Note for S3FT9MD/MC, MF/MR/MS, MH/MV/MG, référence SAN_S3FT9MD_MF_MH_v2.8, version 2.8, daté du 5 juillet 2018, *SAMSUNG ELECTRONICS CO. LTD.* ; - S3FT9MH/MV/MG Chip Delivery Specification, référence S3FT9MH_DV22, révision 2.2, daté de mars 2017, *SAMSUNG ELECTRONICS CO. LTD.* ; - Bootloader User's Manual for S3FT9xx Family Products, référence S3FT9xx_80nm_BootloaderSpecification_v2.4, version 2.4, daté du 23 mars 2017, *SAMSUNG ELECTRONICS CO. LTD.* ; - Architecture Reference: SecuPalm CPU Core, version AR14, daté du 3 mars 2011, *SAMSUNG ELECTRONICS CO. LTD.*
[CER]	Rapport de certification ANSSI-CC-2018/33, "S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Library including specific IC Dedicated software". Certifié par l'ANSSI sous la reference ANSSI-CC-2018/33 le 22 août 2018.
[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.*

Annexe 2. 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 3.0, avril 2019.
[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.