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-2017/24

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

Paris, le 11 mai 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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-2017/24

Nom du produit

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

Référence/version du produit

Référence, Version

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 à

“Package 1: Loader dedicated for usage in Secured Environment only”
“Package 2: Loader dedicated for usage by authorized users only”

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 6 augmenté

ASE_TSS.2

Développeurs

Samsung Electronics Co. Ltd.

17 Floor, B-Tower, 1-1, Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do 445-330
Corée du Sud

Trusted Labs

5, rue du Baillage
78000 Versailles,
France

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 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit 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 le microcontrôleur « S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software », référence S3FT9MH/S3FT9MV/S3FT9MG_rev0-1_SW10-49-50-70-10-103-202_GU113-16-005-201-133-24-22-24-14, 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 les packages « *Loader dedicated for usage in secured environment only* » et « *Loader dedicated for usage by authorized users only* ».

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 non prédictibles.

1.2.3. Architecture

Les produits sont constitués des éléments suivants :

- 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*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
    - de bibliothèques pour la génération de nombres aléatoires *DTRNG FRO library*, et *EHP DTRNG FRO library* ;
    - d'une bibliothèque pour la cryptographie asymétrique *Secure RSA/ECC library* ; cette bibliothèque utilise l'accélérateur *TORNADO-E ;*
    - d'un logiciel *Secure Boot Loader* 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].

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire située à l'offset 0x400000 :

- identification des microcontrôleurs :
    - 0x1611, 0x161F et 0x1610 désignant respectivement les modèles S3FT9MH, S3FT9MV et S3FT9MG ;
- révision :
    - 0x00, 0x01 pour respectivement la révision 0 et la révision 1, fabriquées sur le site Giheung/plant6, par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :
    - *Test ROM Code* : 0x10 pour la version 1.0, par lecture d'un octet à l'adresse 0x40002B ;
    - *Secure Boot loader* : 0x49, 0x50 pour respectivement la version 4.9 (pour la révision 0 du microcontrôleur) et la version 5.0 (pour la révision 1 du microcontrôleur), par lecture d'un octet à l'adresse 0x400030 ;

L'identification des bibliothèques se fait par des fonctions spécifiques :

- *Secure RSA/ECC library* : « PKA_Lib_CE1_v1.03 » ou « PKA_Lib_CE1_v2.02 » pour respectivement les versions 1.03 et 2.02, par lecture en ASCII des données retournées par la fonction *PKA_library_version_info* ;
- *DTRNG FRO Library* : 0x0700 pour la version 7.0, par lecture des 1re et 2de valeurs hexadécimales retournées par la fonction *DTRNG_version* ;
- *EHP DTRNG FRO Library Version* : 0x0100 pour la version 1.0, par lecture des 1ere et 2de valeurs hexadécimales retournées par la fonction *DTRNG_version*.

Cette procédure d'identification est décrite dans le guide « *Chip Delivery Specification* » (voir [GUIDES]).

1.2.5. Cycle de vie

Le cycle de vie du produit peut être représenté par le schéma suivant :

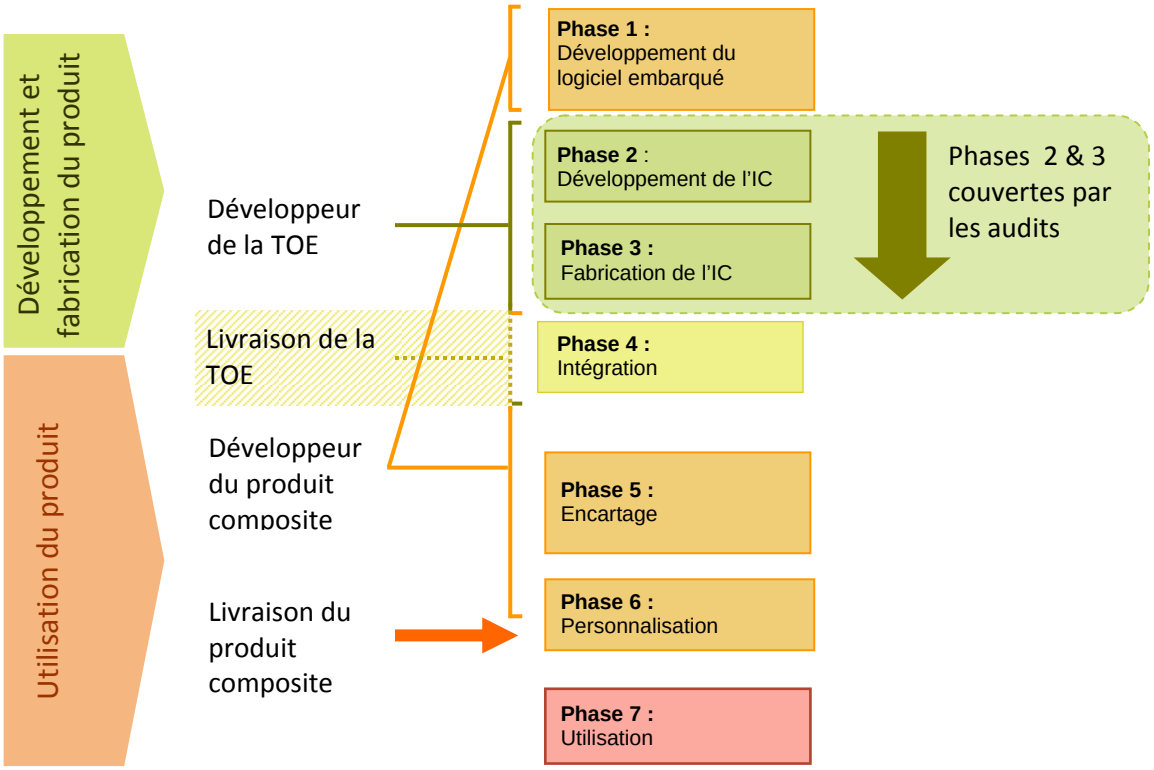

Figure 1 : Cycle de vie du produit

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.

La TOE est développée sur les sites suivants :

Nom du Site	Adresse	Fonction
TRUSTED LABS	*TRUSTED LABS* 5, rue du Baillage 78000 Versailles France	Phase 2 : fournitures spécifiques pour ADV_SPM.1 & ADV_INT.3 Co-édition de la Cible de Sécurité
HWASUNG PLANT/ DSR BUILDING	1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, Corée du Sud San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 2 : *Smart Card Design Center*
HWASUNG PLANT/ DSR BUILDING		Phase 3 : *Test program development*
HWASUNG PLANT/ NRD BUILDING		Phase 3 : *Mask Shop*
PKL PLANT	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : *Mask Shop*
GIHEUNG PLANT/ LINE 6, LINE S1	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do Corée du Sud	Phase 3 : *IC Fabrication*
GIHEUNG PLANT/ LINE 1,LINE 2		Phase 3 : *Testing, Wafer Stock, Inking, Back Side Grinding*
HANAMICRON PLANT	95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 & 4: *Grinding/Sawing/Package testing*
TESNA PLANT	450-2 Mogok-Dong, Pyeungtaek City, Gyeonggi, Corée du Sud	Phase 3 : *Wafer Testing*
ASE KOREA	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, SIP module assembly*
ETERNAL PLANT	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 3&4 : *Sawing, COB, Packaging, Warehouse*
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*
ONYANG PLANT LINE2, LINE6, WAREHOUSE	San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : *Wafer Stock,Grinding, Sawing, Packaging, Package Testing, Warehouse*

Le produit comporte une gestion de son cycle de vie, prenant la forme de deux configurations :

- configuration « *TEST mode* » : à la fin de la fabrication, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM. Cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration « *NORMAL mode* » ;
- configuration « *NORMAL mode* », qui supporte deux sous-modes d'exécution pour le processeur :
  - le sous-mode « *PRIVILEGE* », activé lors de l'exécution de routines d'interruption, est un mode d'exécution interne au processeur qui permet d'accéder aux registres de contrôle et de sécurité et de configurer la MPU (*Memory Protection Unit*) ; lorsque le processeur a terminé l'exécution de la routine, il retourne automatiquement en mode « *USER* » ;
  - le sous-mode « *USER* » : mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible.

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 4** [CC], et à la méthodologie d'évaluation définie dans le manuel CEM [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 sous la référence [ANSSI-CC-2016/59].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 avril 2017, 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

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.

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* » (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 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software » 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 composant 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 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 puces 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 :

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[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 :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, la Pologne, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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 : - S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated software, ST (Security Target), version 4.5, 27 mars 2017, Samsung. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated software, ST (Security Target) Lite, version 3.2, 27 mars 2017, Samsung.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) - LETI.CESTI.KLA7R2.FULL.001, version 1.0, 31 mars 2017, 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), LETI.CESTI.KLA7R2.COMPO.001, version 1.0, 31 mars 2017, CEA-LETI.
[CONF]	Liste de configuration du produit : - Klallam7R2 Life Cycle Definition (Class ALC_CMC.5/CMS.5), version 3.2, 27 mars 2017, Samsung.

[GUIDES]	Guides du produit : - *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note*, version 1.13, 17 mars 2017, Samsung ; - *S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, revision 1.6, 27 mars 2017,* Samsung ; - *S3FT9XX, 16-bit CMOS Microcontroller for Smart Card, User's Manual,* révision 1.33, mars 2017, Samsung ; - *Security Application Note for S3FT9MD/MC,MF/MT/MS, MH/MV/MG*, version 2.4, 10 mars 2017, Samsung ; - *PKA Library API Manual (PKA_Lib_CE1_APIManual_v0.05),* 21 mars 2017, Samsung ; - *RSA/ECC Library API Manual (CE1 RSA ECC Library API Manual v2.01), 21 mars 2017, Samsung ;* - *S3FT9MH /MV /MG Chip Delivery Specification*, revision 2.2, mars 2017, Samsung ; - *Bootloader User's Manual for S3FT9xx Family Products*, version 1.9, 9 juin 2015, Samsung ; - *80nm FSID Devices Bootloader Specification Appendix,* revision 2.4, 23 mars 2017, Samsung; - *SecuCalm CPU CORE, Architecture Reference*, référence: S3xT9xx_AR14_SecuCalmCore, version AR14, Samsung.
[PP0084]	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-CC-PP-0084-2014 *le 19 février 2014*.
[ANSSI-CC-2016/59]	Rapport de certification ANSSI-CC-2016/59, S3FT9MH / S3FT9MV / S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library, 2 septembre 2016, ANSSI.

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 de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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.
[AIS31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 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.