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-2014/37

Microcontrôleurs SAMSUNG S3FT9MD et S3FT9MC Revision 0

Paris, le 11 juillet 2014

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

[Original signé]
Guillaume POUPARD

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2014/37

Nom du produit

Microcontrôleurs SAMSUNG S3FT9MD et S3FT9MC

Référence/version du produit

Revision 0

Conformité à un profil de protection

[PP0035] : Security IC Platform Protection Profile Version 1.0

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

Samsung Electronics Co. Ltd.
17th floor, B-Tower
1-1, Samsungjeonja-ro, Hwaseong-si
Gyeonggi-do 445-330 South Korea
COREE DU SUD

Commanditaire

Samsung Electronics Co. Ltd.
17th floor, B-Tower
1-1, Samsungjeonja-ro, Hwaseong-si
Gyeonggi-do 445-330 South Korea
COREE 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 EAL4.

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

Les produits évalués sont les « Microcontrôleurs SAMSUNG S3FT9MD et S3FT9MC, révision 0 » développés par Samsung Electronics Co. Ltd.

Les deux produits faisant l'objet de ce certificat diffèrent uniquement par la quantité de mémoire FLASH disponible. Les tailles de mémoire FLASH correspondant à chaque modèle sont précisées dans le chapitre suivant.

Le produit est identique à celui précédemment certifié sous la référence [CER-2013/58]. Seule une modification du périmètre de la TOE justifie la présente réévaluation : le DTRNG évalué, appelé ici DTRNG FRO, fait appel à un générateur matériel qui était déjà présent sur le produit certifié mais ne faisait pas partie de la TOE.

Par ailleurs deux nouveaux sites sont ajoutés au cycle de vie du produit (voir chapitre 1.2.4).

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, transports, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit

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 [PP0035].

1.2.1. 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 :
  - 0x160D, désignant le modèle S3FT9MD ou 0x160C, désignant le modèle S3FT9MC, par lecture de deux octets à l'adresse 0x400004 ;
- révision :
  - 0x00 pour la révision 0 par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :
  - *DTRNG library* : 0x05 pour la version 5.0 par lecture d'un octet à l'adresse 0x40002F ;
  - *Test ROM Code* : 0x10 pour la version 1.0 par lecture d'un octet à l'adresse 0x40002B ;

- *Secure Boot loader* : 0x43 pour la version 4.3 par lecture d'un octet à l'adresse 0x400030.

Ces éléments ont été vérifiés par l'évaluateur.

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 génération de nombres non prédictibles.

1.2.3. Architecture

Les microcontrôleurs S3FT9MD et S3FT9MC sont constitués des éléments suivants :
- une partie matérielle comprenant :
  - un processeur SecuCalm RISC 16 bits ;
  - des mémoires :
    - 32 Ko de ROM utilisateur (12 Ko supplémentaires sont occupés par les logiciels de tests) ;
    - 4 Ko de RAM ;
    - 160 Ko et 136 Ko de FLASH, respectivement pour les modèles S3FT9MD et S3FT9MC ;
  - 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 et sans-contact (UART ISO 7816 et ISO 14443), génération de nombres aléatoires – DTRNG (*Digital True Random Number Generator*[1]) et coprocesseurs cryptographiques DES[2] et AES ;
- 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 ;
  - d'une bibliothèque pour le DTRNG ;
  - d'un *Secure Boot Loader* (utilisant le coprocesseur AES) permettant le chargement sécurisé du code utilisateur.

[1] Générateur physique de nombres aléatoires.
[2] Seul le mode de chiffrement 3DES est dans le périmètre de l'évaluation.

1.2.4. Cycle de vie

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

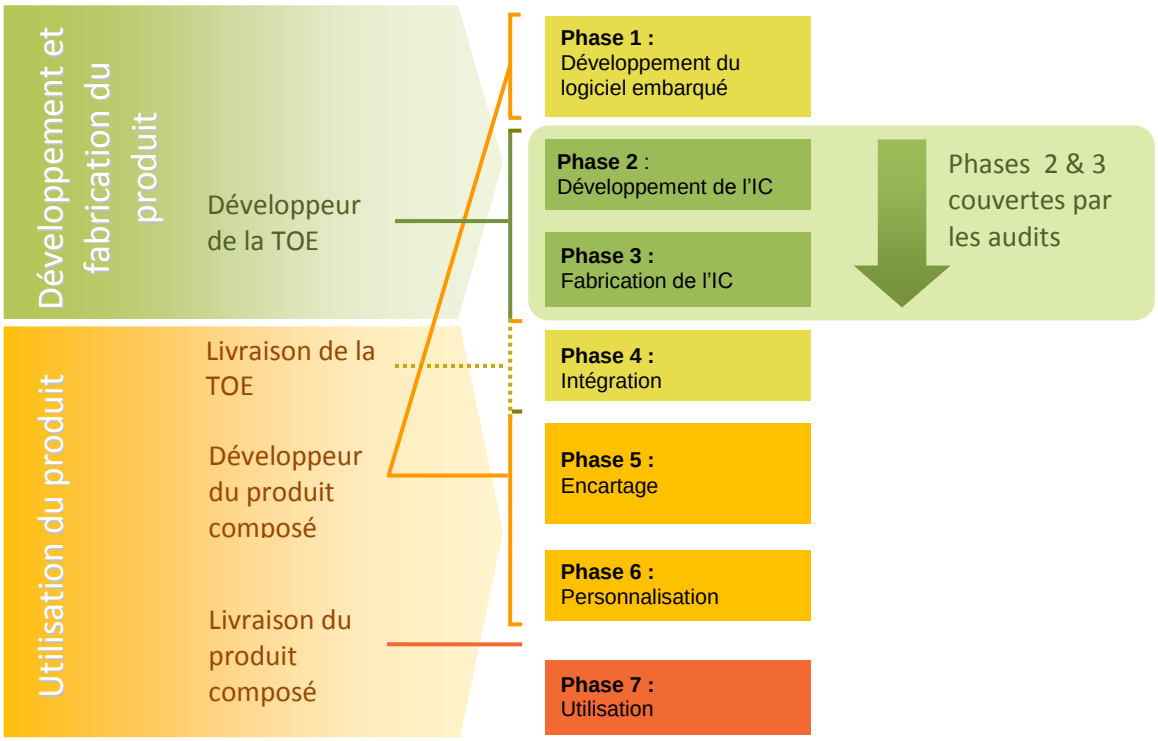

Figure 1 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de wafers en début de 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 :

Giheung Plant

San 24, Nongseo-Dong, Giheung-Gu,
Yongin-City, Gyeonggi-Do 446-711
République de Corée

Hwasung Plant

San #16, Banwol-Dong
Hwasung-City, Gyeonggi-Do
République de Corée

PKL Plant

493-3, Sungsung-Dong
Cheonan-City, Choongcheongnam-Do
République de Corée

TESNA Plant

No. 450-2 Mogok-Dong,
Pyeungtaek-City, Gyeonggi-Do
République de Corée

HANAMICRON Plant

#95-1 Wonnam-Li, Umbong-Myeon
Asan-City, Choongcheongnam-Do
République de Corée

Eternal Plant

No.1755, Hong Mei South Road
Shanghai
République Populaire de Chine

ChangFeng Plant

No. 818, Jin Yu Road
Jin Qiao Export Processing Zone, Pudong,
Shanghai
République Populaire de Chine

ASE Korea

Sanupdanjigil 76, Paju
République de Corée

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.

1.2.5. Configuration évaluée

Le certificat porte sur le microcontrôleur et les bibliothèques logicielles qu'il embarque tels que définis au 1.2.1. 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 1.2.4, le produit évalué est celui obtenu à l'issue de la phase 3.

De même que pour l'évaluation initiale, le modèle S3FT9MD a été utilisé par l'évaluateur pour mener ses tests ; les résultats sont applicables indifféremment aux deux modèles faisant l'objet de ce certificat.

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].

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 [CC 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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 novembre 2013, 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 les référentiels techniques 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 visé.

2.4. Analyse du générateur d'aléas

Le produit embarque 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. 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.

Le DTRNG a en outre fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation : il atteint le niveau « P2 – *High level* » (voir [RTE-AIS31]).

Les guides associés au générateur d'aléa, notamment : « *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note* » et « *Security Application Note for S3FT9MD/MC,MF/MT/MS, MH/MK/MG* » (voir [GUIDES]) doivent être scrupuleusement appliqués.

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 les produits « Microcontrôleurs SAMSUNG S3FT9MD et S3FT9MC, révision 0 » soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans leur 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 des produits « Microcontrôleurs SAMSUNG S3FT9MD et S3FT9MC » 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.

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. 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 EAL4 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, 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, 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							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**	Semi-formal 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_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**	1	**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 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3FT9MD / S3FT9MC 16-bit RISC Microcontroller for Smart Card*, référence: ST Klallam4 R v2.2, version 2.2, Samsung. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Project S3FT9MD/MC - Security Target Lite of Samsung 16-bit RISC Microcontroller for Smart Card*, référence: ST Lite S3FT9MD_MC v1.1, version 1.1, Samsung.
[RTE]	Rapport technique d'évaluation : - *KLALLAM4R Evaluation Technical Report : RTE*, référence: LETI.CESTI.KLA4R.ANSSI.001, version 1.0, CEA LETI. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *KLALLAM4R Evaluation Technical Report Lite : RTE*, référence: LETI.CESTI.KLA4R.ANSSI.002, version 1.0, CEA LETI.
[CONF]	Liste de configuration du produit : - Project < KLALLAM4 R> Life Cycle Definition (Class ALC_CMC.4/CMS.5), référence : ALC_CMC_CMS_Klallam4R_V1.5, version 1.5, Samsung.
[GUIDES]	Guides du produit : - *Security Application Note for S3FT9MD/MC,MF/MT/MS, MH/MK/MG*, référence : SAN_S3FT9MD_MF_MH_v1.3, version 1.3, Samsung ; - *S3FT9MD/MC Chip Delivery Specification*, référence: S3FT9MD_DV11, version 1.1, Samsung ; - *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note*, référence : S3FT9XX_DTRNG_FRO_AN_v1.4, version 1.4, Samsung ; - *SecuCalm CPU CORE, Architecture Reference*, référence : S3xT9xx_AR14_SecuCalmCore, version AR14, Samsung ; - *Bootloader User's Manual for S3FT9xx Family Products*, référence : S3FT9xx_80nm_BootloaderSpecification_v1.5, version 1.5, Samsung ; - *80nm FSID Devices Bootloader User's Manual Guide Errata*, référence : TN03_80nm FSID Devices_for_Bootloader_User's_Manual_Guide_20131122, version 3.00, Samsung ; - *User's Manual*, référence: S3FT9XX_UM_REV1.10, version 1.10, Samsung.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI sous la référence BSI-PP-0035-2007.*

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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, revision 4, ref CCMB-2012-09-004.
[CC IC]	Common Criteria Supporting Document – Mandatory Technical Document – The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]	Mandatory Technical Document – Application of attack potential to smart-cards, JIWG, version 2.9, January 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
[AIS 31]	*Functionnality classes and evaluation methodology for physical random number generator*, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).