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-2015/42

Microcontrôleur SAMSUNG S3FT9FA revision 0

S3FT9FA _rev0_SW10-45-60-GU111-12-18-12-19-14-20-04

Paris, le 15 septembre 2015

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

[ORIGINAL SIGNE]

Contre-amiral
Dominique RIBAN

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-2015/42

Nom du produit

Microcontrôleur SAMSUNG S3FT9FA révision 0

Référence/version du produit

S3FT9FA _rev0_SW10-45-60-GU111-12-18-12-19-14-20-04

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 february 2014

avec conformité à

"Package 1: Loader dedicated for usage in Secured Environment only"

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(s)

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 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 « Microcontrôleur SAMSUNG S3FT9FA, révision 0 » 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,...) 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 »*.

1.2.2. Identification du produit

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

Comme décrit dans [GUIDE], la version certifiée du produit est identifiable par les éléments suivants :

- Le modèle S3FT9FA est reconnu par la valeur attendue 0x0F0A en lecture de deux octets à l'adresse 0x400004 ;
- La révision 0 est reconnue par la valeur attendue 0x00 en lecture d'un octet à l'adresse 0x40002A ;
- La version 1.0 du logiciel dédié « Test ROM » est reconnue par la valeur attendue 0x10 en lecture d'un octet à l'adresse 0x40002B ;
- La version 4.5 du logiciel dédié « Boot loader » est reconnue par la valeur attendue 0x45 en lecture d'un octet à l'adresse 0x400030 ;
- La version 6.0 de la bibliotheque « DTRNG FRO » est reconnue par la valeur attendue 0x0600 en réponse à l'appel de fonction « DTRNG_VERSION FUNCTION ».

1.2.3. 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 TripleDES ;
- le support à la génération d'aléa.

1.2.4. Architecture

Le produit est principalement constitué les éléments suivants :

– une partie matérielle comprenant :
  - o des mémoires : FLASH de 120ko, RAM de 4ko, User ROM de 32ko, Flash special area de 768 octets ;
  - o un processeur SecuCalm RISC 16 bits ;
  - o 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 ;
  - o un coprocesseur cryptographique TripleDES ;
  - o deux générateurs d'aléa physique : DTRNG FRO et BPRNG ;
  - o un module de gestion des entrées/sorties en mode contact ;
– une partie logicielle composée :
  - o des logiciels de test du microcontrôleur (*Test ROM*) embarqués en mémoire ROM et ne faisant pas partie de la TOE ;
  - o d'une bibliothèque nécessaire à l'utilisation du module DTRNG FRO ;
  - o d'un *Secure Boot Loader* permettant le chargement sécurisé du code utilisateur.

1.2.5. Cycle de vie

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

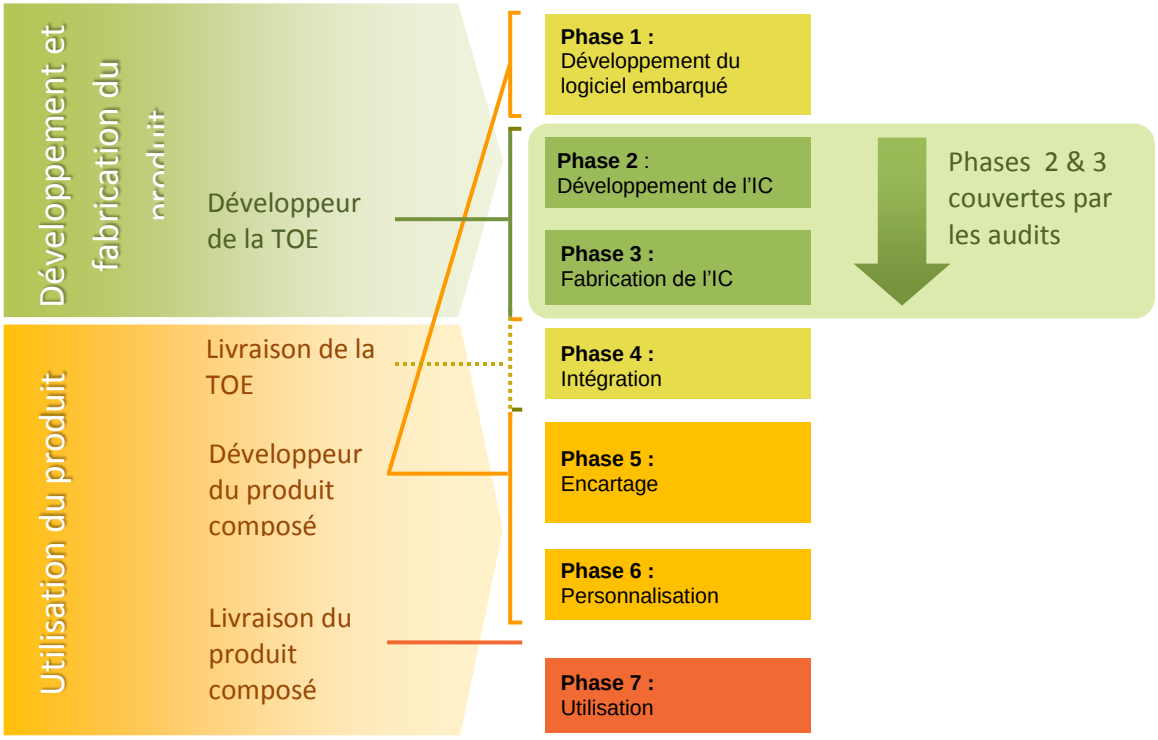

Figure 1 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de wafers en début de phase 4, ou bien optionnellement sous forme de micro-modules en fin 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 :

Hwasung Plant (bat. DSR)

1, Samsungjeonja-ro (Banwol-Dong)
Hwasung-City, Gyeonggi-Do
République de Corée

Hwasung Plant (bat. NRD)

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

Giheung Plant (Line 1, 2, 6 S1)

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

Onyang Plant (Warehouse, Line 2, Line 6)

San#74, Buksoo-Ri, Baebang-Myun,
Asan-City, Choongcheongnam-Do,
République de Corée

PKL Plant

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

HANAMICRON Plant

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

Inesa Plant

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

Eternal Plant

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

TESNA Plant

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

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* », avant livraison du produit ;
- 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.

Dans la cible de sécurité, le développeur a opté pour la conformité au « *Package 1 : loader dedicated for usage in secured environment only* » du profil de protection [PP0084].

1.2.6. Configuration évaluée

Le certificat porte sur le microcontrôleur et les bibliothèques logicielles qu'il embarque 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 ou à l'issue de la phase 4.

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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 27 août 2015, 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 qui a fait l'objet d'une analyse par le CESTI, appelé DTRNG FRO, incluant un retraitement de lissage, et utilisable à travers une bibliothèque fournie. Les règles RègleArchiGVA-1 et RègleArchiGVA-2 ainsi que la recommandation RecomArchiGVA-1 de [REF] s'avèrent respectées.
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, comme indiqué dans « *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note* » (voir [GUIDES]).

Ce générateur physique d'aléa a en outre fait l'objet d'une évaluation selon l'ancienne version de la méthodologie AIS31 (voir [AIS 31]) : il atteint le niveau « P2 – *High level* ».

Les guides associés au générateur d'aléa, notamment : « *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note* » et « *Security Application Note for*

S3FT9FD/FC/FB, PF/PT/PS, PE, FA» (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 le produit « Microcontrôleur SAMSUNG S3FT9FA, révision 0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

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

Ce certificat donne une appréciation de la résistance du produit « Microcontrôleur SAMSUNG S3FT9FA, révision 0 » 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. 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, 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**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	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 S3FT9FA 16-bit RISC Microcontroller for Smart Card, version 2.7, 21 août 2015, Samsung. 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 S3FT9FA 16-bit RISC Microcontroller for Smart Card, version 2.3, 26 août 2015, 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 february 2014.
[GUIDES]	Guides du produit : - Security Application Note for S3FT9FD/FC/FB, PF/PT/PS, PE, FA, référence : SAN_S3FT9FD_PF_PE_FA_v1.8, version 1.8, novembre 2014, Samsung ; - S3FT9FA Chip Delivery Specification, reference : S3FT9FA_DV12, version 1.2, juin 2014, Samsung **;** - S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, référence : S3FT9XX_DTRNG_FRO_AN_v1.11, version 1.11, juin 2015, 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_v1.9, version 1.9, juin 2015, Samsung ; - Bootloader Specification Apendix : 80 nm FSID Devices, reference : S3FT9xx_80nm_BootloaderSpecification_Appendix02, version 2.0, juin 2015, Samsung ; - S3FT9XX 16-Bit CMOS Microcontroller User's Manual, référence: S3FT9XX_UM_REV1.20, version 1.20, septembre 2014, Samsung ; - User's Manual Errata for User's Manual Revision 1.20, reference : S3FT9XX_UM1.2, version 0.40, June 2015, Samsung

[CONF]	Liste de configuration du produit : - Life Cycle Definition (Class ALC_CMC.4/CMS.5), référence : Klallam6R_ALC_CMC_CMS_V2.4, version 2.4, 25 août 2015, Samsung.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – KLALLAM6-R, LETI.CESTI.KLA6R.FULL.001 - V1.1, 27 août 2015, 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) – KLALLAM6-R, LETI.CESTI.KLA6R.COMPO.001 - v1.1, 27 août 2015, CEA LETI.

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, 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.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31, version 1, 25 septembre 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).

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