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-2015/20

Microcontrôleur SAMSUNG S3FW9F4
Revision 0

Paris, le 22 mai 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2015/20

Nom du produit

Microcontrôleur SAMSUNG S3FW9F4 Revision 0

Référence/version du produit

S3FW9F4 _Rev0_SW10-10_GU022-13-05-02-A

Conformité à un profil de protection

None

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.4

Développeur

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

Commanditaire

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

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

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 SAMSUNG S3FW9F4, 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. Ce microcontrôleur est principalement dédié au marché des cartes SIM. Les logiciels applicatifs qui seront installés sur celui-ci 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 s'inspire du profil de protection [PP0084].

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 :

- identification du microcontrôleur :
  - 0x0F04, désignant le composant S3FW9F4, par lecture de deux octets aux adresses 0x3FFD04-0x3FFD05 ;
- révision :
  - 0x00 pour la révision 0 par lecture d'un octet à l'adresse 0x3FFD2A ;
- identification des logiciels embarqués :
  - *DTRNG (Digital True Random Number Generator[1]) library :* la fonction DTRNG_version renvoie 2 octets identifiant la version du logiciel (voir [GUIDES]) *;*
  - *Test ROM Code* : 0x10 pour la version 1.0 par lecture d'un octet à l'adresse 0x3FFD2B.

Ces éléments ont été vérifiés par l'évaluateur.

1.2.1. 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 à la génération de nombres non prédictibles.

[1] Générateur physique de nombres aléatoires.

1.2.2. Architecture

Le microcontrôleur S3FW9F4 est constitué des éléments suivants :

- une partie matérielle comprenant :
  - un processeur 32 bits SC000 ;
  - des mémoires :
    - 2 Ko de ROM occupés par les logiciels de tests ;
    - 5 Ko de RAM ;
    - 228 Ko de FLASH ;
  - des modules de sécurité : surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, bouclier actif, etc ;
  - des modules fonctionnels : gestion des entrées/sorties en mode contact (ISO 7816-3), génération de nombres aléatoires (DTRNG), *timer* 16 bits ;
- une partie logicielle composée :
  - d'une bibliothèque pour la génération de nombres aléatoires ;
  - des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE.

1.2.3. Cycle de vie

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

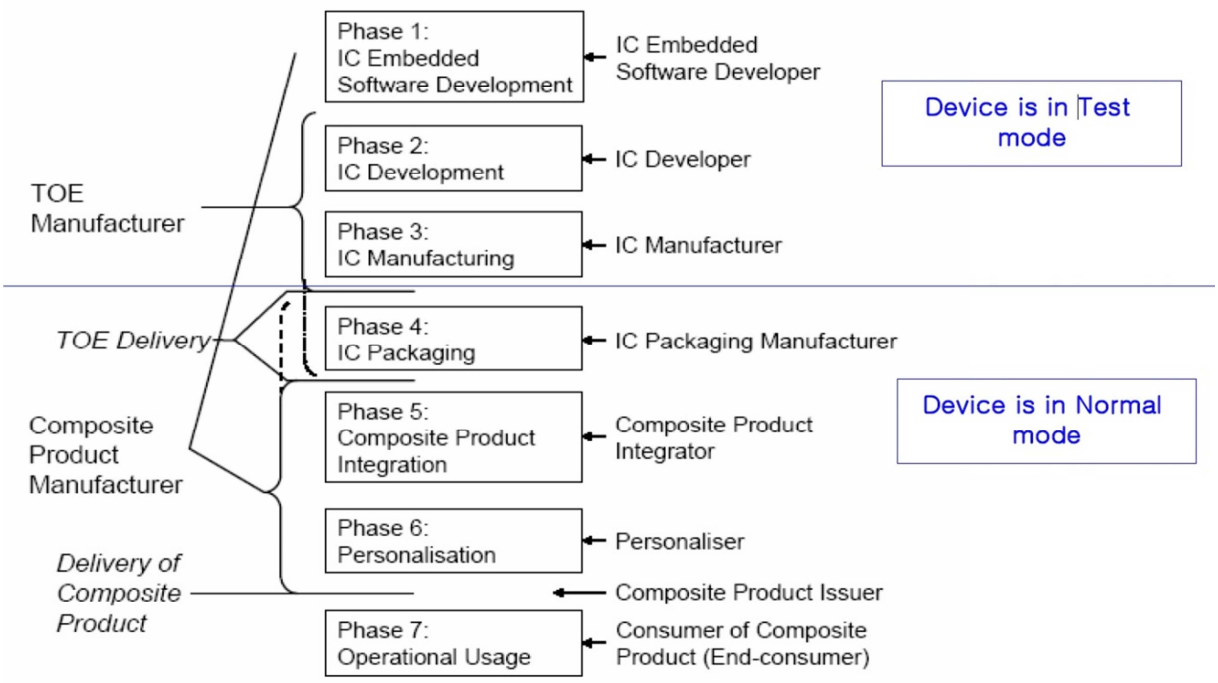

Figure 1 : Cycle de vie du produit

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 :

- la conception du circuit ;
- le développement du logiciel dédié.

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

- l'intégration et la fabrication du masque ;
- la fabrication du circuit ;
- le test du circuit ;
- la préparation ;
- la pré-personnalisation si nécessaire.

La TOE est développée sur les sites suivants :

Giheung Plant

Line 6, S1 San #24, Nongseo-Dong,
Giheung-Gu,
Yongin-City, Gyeonggi-Do
République de Corée

Giheung Plant

LCD Building San #24, Nongseo-Dong,
Giheung-Gu,
Yongin-City, Gyeonggi-Do
République de Corée

Hwasung Plant

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

Hwasung Plant

DSR building 1,Samsungjeonja-ro
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

Giheung Plant

Line 2 San #24, Nongseo-Dong, Giheung-Gu,
Yongin-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

Inesa Plant

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

ASE Korea

76, Sanupdanjigil, Paju-si
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 « *USER* » : mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible ;

- 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* ».

1.2.4. Configuration évaluée

Le certificat porte sur le microcontrôleur et la bibliothèque logicielle DTRNG 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 pas partie du périmètre de l'évaluation.
Au regard du cycle de vie détaillé au chapitre 1.2.3, le produit évalué est celui obtenu à l'issue de la phase 3.

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 [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 15 avril 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 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 incluant un retraitement qui a fait l'objet d'une analyse par le CESTI. Cette analyse montre que ce DTRNG est conforme aux tests statistiques *Test Procedure A* de la méthodologie [AIS 31]. Elle 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.

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 S3FW9F4, révision 0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2 et AVA_VAN.4.

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 S3FW9F4, 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 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 impérativement les recommandations se trouvant dans les guides fournis [GUIDES].

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 4+	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**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic 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	**4**	Problem tracking 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	**1**	Well-defined development tools
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**	**1**	Testing: basic 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	**4**	Moderate vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3FW9F4*, reference : ST Delaware v0.7, version 0.7, March 30th 2015, Samsung.
[RTE]	Rapport technique d'évaluation : - *DELAWARE Evaluation Technical Report : RTE*, référence: LETI.CESTI.DEL.FULL.001, version 1.0, April 15 th 2015, CEA LETI.
[CONF]	Liste de configuration du produit : - Project < DELAWARE> Life Cycle Definition (Class ALC_CMC.4/CMS.4), référence : Delaware_ALC_CMC_CMS_V1.4, version 1.4, March 30 th 2015, Samsung.
[GUIDES]	Guides du produit : - *S3FW9F4 Security Application Note*, référence : SAN_S3FW9F4_Rev_0.5, version 0.5, March 27th 2015, Samsung ; - *S3FW9F4 Chip Delivery Specification*, reference : DeliverySpec_S3FW9F4_Rev_0.2, version 0.2, December 2014, Samsung ; - *S3FW9FX HW DTRNG and DTRNG Library Application Note*, référence : S3FW9FX_DTRNG_Library_AN_v1.3, version 1.3, March 30th 2015, Samsung ; - *S3FW9F4/FC User's Manual*, référence: S3FW9F4_UM_REV0.22, version 0.22, March 2015, Samsung ; - *SC000 Revision: r0p0 technical Reference Manual*, référence: SC000_TechnicalReferenceManual_r0p0, version A, September 3rd 2010, Samsung.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, June 19th, 2014. *Certifié par le BSI sous la référence BSI-PP-0084-2014*.

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.
[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 smart-cards, JIWG, version 2.9, January 2013.
[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 (RGS_B_1), 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).

*Documents du SOG-IS.