



*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-2014/75**

### **SAMSUNG S3FV9QM/S3FV9QK, révision 3**

rev3\_SW10\_25\_11\_30\_GU136\_12\_111\_13\_01\_124 et  
rev3\_SW10\_25\_12\_30\_GU136\_12\_111\_13\_01\_124

*Paris, le 6 novembre 2014*

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

[ORIGINAL SIGNE]  
Guillaume POUPARD



## 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 présumées 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](mailto:certification.anssi@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

**ANSSI-CC-2014/75**

Nom du produit

**SAMSUNG S3FV9QM/S3FV9QK, révision 3**

Référence/version du produit

**rev3\_SW10\_25\_11\_30\_GU136\_12\_111\_13\_01\_124 et  
rev3\_SW10\_25\_12\_30\_GU136\_12\_111\_13\_01\_124**

Conformité à un profil de protection

**[PP0035] : Security IC Platform Protection Profile  
Version 1.0, June 2007, BSI-PP-0035**

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**  
17 Floor, B-Tower, 1-1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-Do, 445-330  
République de Corée

Commanditaire

**SAMSUNG Electronics Co. Ltd**  
17 Floor, B-Tower, 1-1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-Do, 445-330  
République de Corée

Centre d'évaluation

**CEA - LETI**  
17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables



**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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Introduction</i> .....	6
1.2.2. <i>Identification du produit</i> .....	6
1.2.3. <i>Services de sécurité</i> .....	7
1.2.4. <i>– Architecture</i> .....	7
1.2.5. <i>Cycle de vie</i> .....	9
1.2.6. <i>Configuration évaluée</i> .....	11
<b>2. L’EVALUATION .....</b>	<b>12</b>
2.1. REFERENTIELS D’EVALUATION .....	12
2.2. TRAVAUX D’EVALUATION .....	12
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	12
2.4. ANALYSE DU GENERATEUR D’ALEAS .....	12
<b>3. LA CERTIFICATION .....</b>	<b>13</b>
3.1. CONCLUSION .....	13
3.2. RESTRICTIONS D’USAGE .....	13
3.3. RECONNAISSANCE DU CERTIFICAT .....	14
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	14
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	14
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT [CCV3.1R2] .....</b>	<b>15</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>16</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Les produits évalués sont les microcontrôleurs « SAMSUNG S3FV9QM/S3FV9QK, révision 3, références rev3\_SW10\_25\_11\_30\_GU136\_12\_111\_13\_01\_124 et rev3\_SW10\_25\_12\_30\_GU136\_12\_111\_13\_01\_124 » développés par SAMSUNG Electronics Co. Ltd.

La seule différence entre les produits S3FV9QM et S3FV9QK réside dans la taille de la mémoire FLASH : 1280 Ko pour S3FV9QM et 1024 Ko pour S3FV9QK.

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 [PP0035].

### 1.2.2. Identification du produit

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

Les références rev3\_SW10\_25\_11\_30\_GU136\_12\_111\_13\_01\_124 et rev3\_SW10\_25\_12\_30\_GU136\_12\_111\_13\_01\_124 attribuées par le développeur au produit correspondent à la concaténation des numéros de révisions ou versions des éléments cités ci-dessous et des guides sécuritaires.

La version certifiée du produit est identifiable par les éléments suivants :

- microcontrôleur : **SAMSUNG S3FV9QM/S3FV9QK, révision 3** ;
- bibliothèques logicielles : *Boot loader v2.5, Crypto Library v1.1* ou *v1.2* (optionnelle), *DTRNG<sup>1</sup> library v3.0, Test ROM v1.0* (hors cible d'évaluation).

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire FLASH (non effaçable) :

- identification des microcontrôleurs par lecture de deux octets à l'adresse 0x400004 :
  - o **0x1A16** pour S3FV9QM ;
  - o **0x1A14** pour S3FV9QK ;

---

<sup>1</sup> *Digital True Random Number Generator* ou Générateur physique et numérique de nombres aléatoires.

- Version de l'IC : **0x03** (pour la révision 3) par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :
  - o *Test ROM code* : **0x10** pour la révision 1.0 par lecture d'un octet à l'adresse 0x40002B ;
  - o *Boot loader code* : **0x25** pour la révision 2.5 par lecture d'un octet à l'adresse 0x400030 ;
  - o *Crypto Library* : **0x011A** pour la révision 1.1 (support pour les calculs cryptographiques RSA) ou **0x012A** pour la révision 1.2 (support pour les calculs cryptographiques RSA et ECC) par lecture de deux octets à l'adresse 0x40002C ;
  - o *DTRNG library* : **0x03** pour la révision 3 par lecture d'un octet à l'adresse 0x40002F.

Ces éléments ont été vérifiés par l'évaluateur.

### 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, dont les logiciels embarqués, que ce soit en exécution ou lorsqu'elles sont stockées dans les différentes mémoires de la *TOE*<sup>1</sup> ;
- la bonne exécution de services de sécurité fournis par la *TOE* aux logiciels embarqués ;
- le support à la cryptographie à clés symétriques ;
- le support à la cryptographie à clés asymétriques avec la librairie cryptographique optionnelle *Crypto Library* (RSA seul pour la révision 1.1, RSA et ECC pour la révision 1.2) ;
- le support à la génération de nombres non prédictibles.

### 1.2.4. Architecture

Les microcontrôleurs S3FV9QM et S3FV9QK sont constitués des éléments suivants :

- une partie matérielle composée en particulier :
  - o d'un processeur 32 bits *RISC*<sup>2</sup> ;
  - o de mémoires :
    - FLASH dont 512 octets de mémoire spéciale et
      - 1280 Ko pour le S3FV9QM ;
      - 1024 Ko pour le S3FV9QK ;
    - 40 Ko de mémoire ROM dont 32 Ko pour le stockage des programmes utilisateurs et 8 Ko pour le *Test ROM* ;
    - 40 Ko de mémoire RAM dont 35 Ko pour le stockage des données utilisateurs et 5 Ko spécifiques pour le calcul cryptographique ;
    - 512 octets de mémoire DMA RAM ;
  - o de modules de sécurité : unité de protection mémoire (*MPU*<sup>3</sup>), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;

<sup>1</sup> *Target Of Evaluation* ou cible d'évaluation.

<sup>2</sup> *Reduced Instruction Set Computer* ou processeur à jeu d'instruction réduit.

<sup>3</sup> *Memory Protection Unit* ou unité de protection mémoire.

- de modules fonctionnels : gestion des entrées/sorties en mode contact (interfaces ISO 7816 et SWP<sup>1</sup>), générateur de nombre aléatoire, crypto-processeurs Triple-DES et AES ainsi qu'un accélérateur cryptographique TORNADO-E pour le support d'algorithmes cryptographiques à clés asymétriques ;
- une partie logicielle comprenant :
  - un logiciel *Test ROM* (hors cible d'évaluation), utilisé par le développeur avant la livraison du produit, inaccessible à l'utilisateur après livraison ;
  - un logiciel *Secure Boot Loader*, permettant à l'utilisateur de charger son code en mémoire FLASH ;
  - une *Crypto Library* et une *DTRNG Library*, permettant à l'utilisateur de réaliser des calculs RSA et ECC ou de générer des nombres aléatoires.

La figure suivante présente l'architecture du produit :

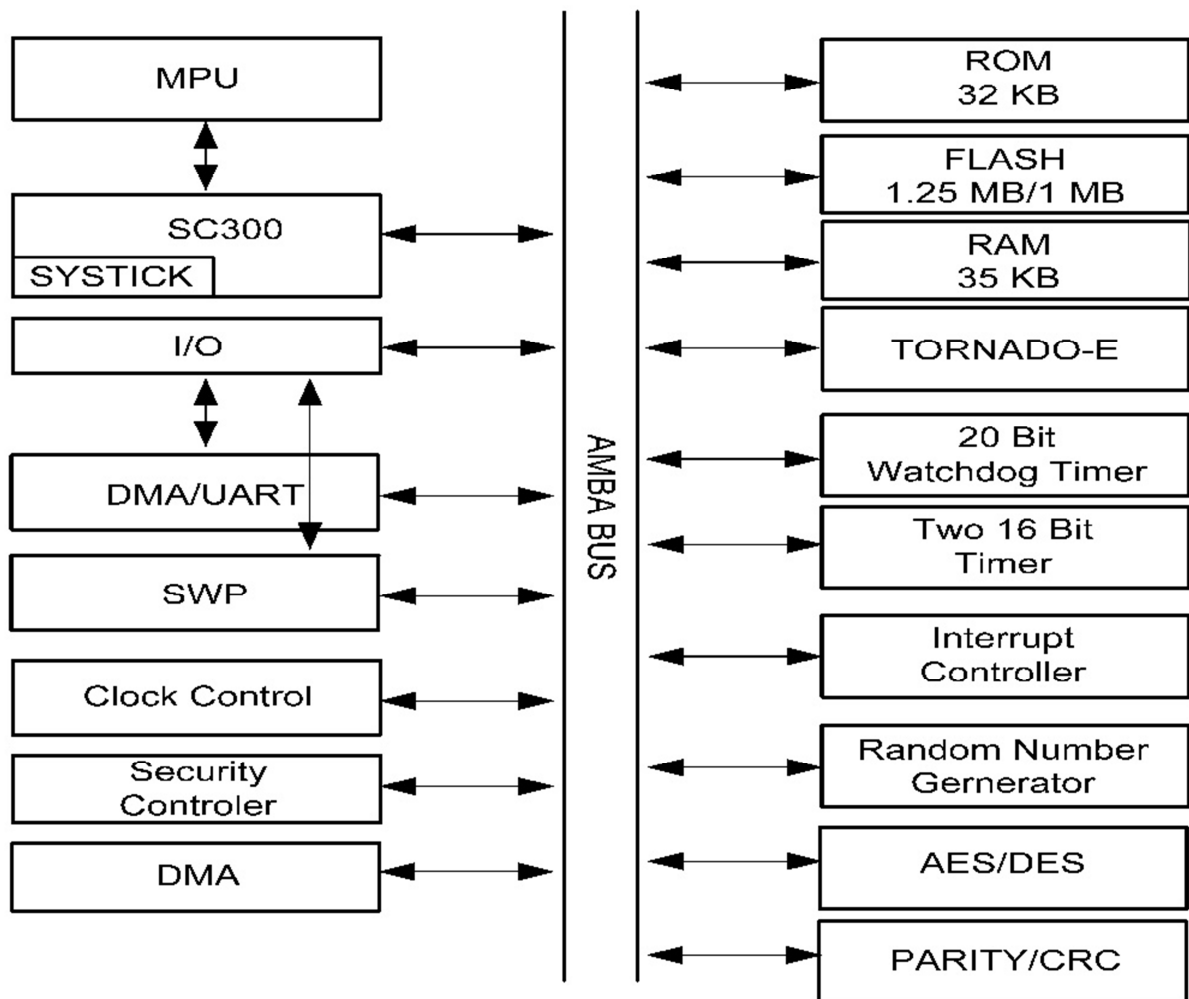


Figure 1 : Architecture du produit

<sup>1</sup> Single Wire Protocol ou protocole simple connexion.



### 1.2.5. Cycle de vie

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

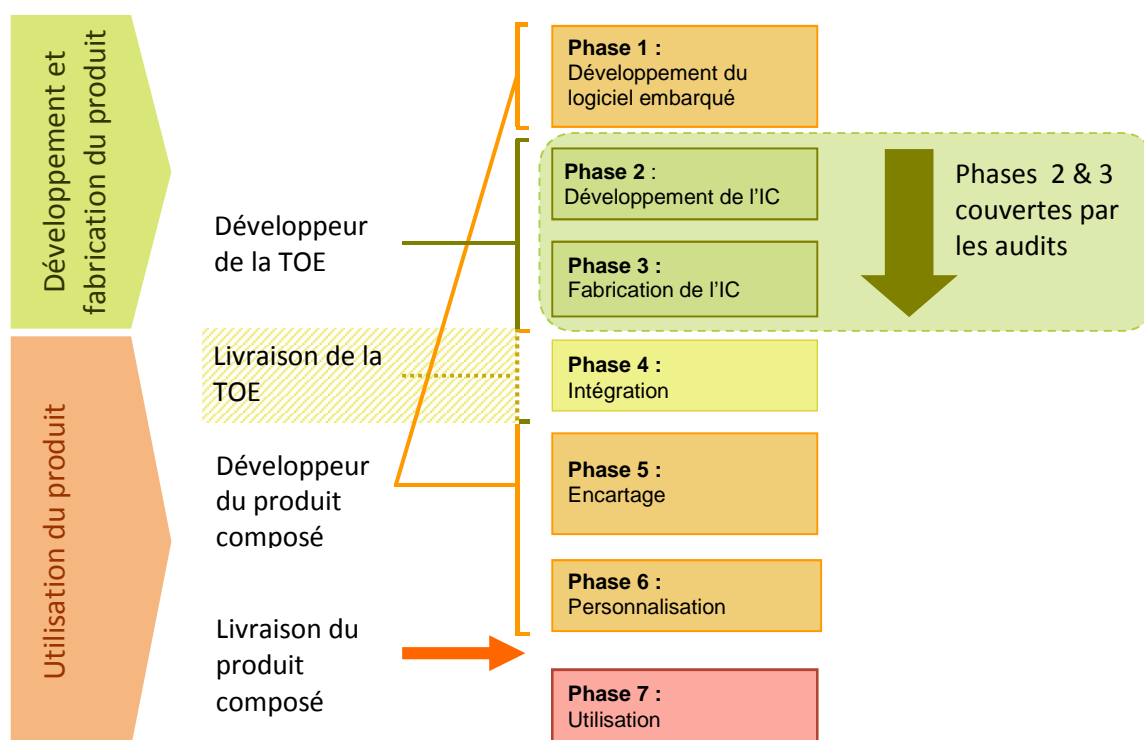


Figure 2 : Cycle de vie du produit

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.

Les produits sont développés sur les sites suivants :

- site de conception :

**Hwasung Plant / DSR Building**  
 Samsungjeonja-Ro (Banwol-Dong) 1  
 Hwasung-City, Gyeonggi-Do,  
 République de Corée

- site de programme de tests  
**Giheung Plant / SR2 Building**  
San #24, Nongseo-Dong, Giheung -Gu  
Yongin-City, Gyeonggi-Do  
République de Corée
  
- site de fabrication des masques :  
**Giheung Plant / LCD Building**  
San #24, Nongseo-Dong, Giheung -Gu  
Yongin-City, Gyeonggi-Do  
République de Corée
  
- site de préparation des masques :  
**Hwasung Plant / NRD Building**  
San #16, Banwol-Dong  
Hwasung-City, Gyeonggi-Do  
République de Corée
  
- site de fabrication des *wafers* :  
**Giheung Plant / Line 6**  
San #24, Nongseo-Dong, Giheung -Gu  
Yongin-City, Gyeonggi-Do  
République de Corée
  
- site de test des *wafers* :  
**Tesna Plant**  
450-2, Mogok-Dong  
Pyeuntaek-City, Gyeonggi-Do  
République de Corée
  
- site de fabrication de test et de stockage des *wafers* :  
**Giheung Plant / Line 2**  
San #24, Nongseo-Dong, Giheung -Gu  
Yongin-City, Gyeonggi-Do  
République de Corée
  
- site de conditionnement des *wafers* :  
**Onyang-Plant et Onyang-Plant/Line2**  
San #74, Buksoo-Ri, Baebang-Myun  
Asan-City, Choongcheongnam-Do  
République de Corée
  
- site externe de fabrication des masques :  
**PKL Plant**  
493-3, Sungsung-Dong, Cheonan-City  
Choongcheongnam-Do  
République de Corée

- site de sciage et polissage des *wafers* :  
**HANAMICRON Plant**  
#95-1 Wonnam-Li, Umbong-Myeon, Asan-City  
Choongcheongnam-Do  
République de Corée
  
- site de sciage et polissage des *wafers* :  
**ASE Korea**  
Saneopdanji-gil 76, Paju-Si, Gyeonggi-Do  
République de Corée
  
- site de stockage, sciage et polissage des *wafers* :  
**ChangFeng Plant**  
No 818 Jin Yu Road, Jin Qiao  
Export Processing Zone Pudong, Shanghai  
République Populaire de Chine
  
- site de conditionnement, stockage et sciage des *wafers* :  
**Eternal Plant**  
No 1755, Hong Mei South Road  
Shanghai  
République Populaire de Chine

Les produits comportent eux-mêmes une gestion de leur cycle de vie, prenant la forme de deux configurations :

- configuration *Test mode* : à la fin de leur 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* : mode comprenant deux sous-modes :
  - o mode « privilégié » : sous-ensemble du mode *Normal mode*, réservé principalement au fonctionnement interne du microcontrôleur ;
  - o mode « non privilégié », dit mode utilisateur : mode final d'utilisation du microcontrôleur, qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce.

### **1.2.6. Configuration évaluée**

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et aux logiciels dédiés embarqués. Toute autre application éventuellement embarquée, notamment les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre d'évaluation.

Le CESTI a jugé que le microcontrôleur S3FV9QM était représentatif des deux microcontrôleurs qui font l'objet de ce rapport de certification et les tests n'ont donc porté que sur ce composant.

## 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 « SAMSUNG S3FV9QM/S3FV9QK, révision 3, références rev3\_SW10-22-11-30\_GU133-12-111-11-01-12 et rev3\_SW10-22-12-30\_GU133-12-111-11-01-12 » certifié en avril 2014 sous la référence [ANSSI-CC-2014/22].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 14 octobre 2014, 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 physique 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 du DTRNG. 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* ».

## 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 « SAMSUNG S3FV9QM/S3FV9QK, révision 3, références rev3\_SW10\_25\_11\_30\_GU136\_12\_111\_13\_01\_124 et rev3\_SW10\_25\_12\_30\_GU136\_12\_111\_13\_01\_124 » 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 « SAMSUNG S3FV9QM/S3FV9QK, révision 3, références rev3\_SW10\_25\_11\_30\_GU136\_12\_111\_13\_01\_124 et rev3\_SW10\_25\_12\_30\_GU136\_12\_111\_13\_01\_124 » 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 un des microcircuits 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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> 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.

<sup>2</sup> 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 [CCv3.1R2]

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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

## Annexe 2. Références documentaires du produit évalué

<p>[ST]</p>	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- Project Cayuse R2, Security Target of Samsung S3FV9QM/S3FV9QK, référence ST Cayuse R2 v4.1, version 4.1, 29 mai 2014, Samsung Electronics Co, Ltd.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- Security Target Lite of Samsung S3FV9QM/S3FV9QK, référence ST Lite S3FV9QM_QK v4.0, version 4.0, 29 mai 2014, Samsung Electronics Co, Ltd.</li> </ul>
<p>[RTE]</p>	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report (full ETR) - CAYUSE-R2, Référence: LETI.CESTI.CAYR2. FULL.001 – V2.2, 14 octobre 2014, CEA-LETI.</li> </ul> <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report: COMPO, référence: LETI.CESTI.CAYR2.COMPO.001 – v2.2 – 14 octobre 2014.</li> </ul>
<p>[CONF]</p>	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- Life Cycle Definition (Class ALC_CMC.4/CMS.5), référence: Cayuse_R2_ALC_CMC_CMS_V4.0, version 4.0, 27 juin 2014, Samsung Electronics Co, Ltd.</li> </ul>
<p>[GUIDES]</p>	<p>Guides du produit :</p> <ul style="list-style-type: none"> <li>- TORNADO-E RSA/ECC Library API Manual, référence: TN_TorE_RSAECC_APIManual_v1.36a, version 1.36a, 7 février 2014, Samsung Electronics Co, Ltd ;</li> <li>- S3FV9XX HW DTRNG and DTRNG library application note, référence : S3FV9XX_DTRNG_AN_v1.2, version 1.2, 26 avril 2012, Samsung Electronics Co, Ltd ;</li> <li>- S3FV9QM/QK 32-Bit CMOS Microcontroller for Smart Card, User's Manual, référence : S3FV9QM_QK_UM_REV1.11, révision: 1.11, 5 décembre 2013, Samsung Electronics Co, Ltd ;</li> <li>- Security Application Note S3FV9QX, référence : SAN_S3FV9QX_v1.3, version 1.3, 2 avril 2014, Samsung Electronics Co, Ltd ;</li> <li>- S3FV9QM/QK Chip Delivery Specification, référence : DeliverySpec_S3FV9QX_Rev_0.1, révision 0.1, mars 2012, Samsung Electronics Co, Ltd ;</li> <li>- Boot Loader Specification for S3FV9QM, référence : S3FV9QM_QK_BootloaderSpecification_v1.2.4, révision : 1.2.4, 6 mai 2014, Samsung Electronics Co, Ltd.</li> </ul>



[ANSSI-CC-2014/22]	Microcontrôleurs «SAMSUNG S3FV9QM/S3FV9QK, révision 3, références rev3_SW10-22-11-30_GU133-12-111-11-01-12 et rev3_SW10-22-12-30_GU133-12-111-11-01-12 ». <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2014/22.</i>
[PP0035]	Security IC Platform Protection Profile version 1.0, 15 juin 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i>

### Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</p>
[CC]	<p>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.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation :          Evaluation Methodology, September 2012, version 3.1, revision 4, ref          CCMB-2012-09-004.</p>
[JIWG IC] *	<p>Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.</p>
[JIWG AP] *	<p>Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.9, January 2013.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of Information Technology Security, July 2014.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.</p>
[REF]	<p>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 <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a>.</p>
[AIS 31]	<p>Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 septembre 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).</p>

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