



*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-2013/03**  
**SAMSUNG S3FV9QM/S3FV9QK, revision 3**

*Paris, le 4 février 2013*

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

Patrick Pailloux  
[ORIGINAL SIGNE]



## 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-2013/03**

Nom et version du produit

**SAMSUNG S3FV9QM/S3FV9QK, revision 3**

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 3**

Niveau d'évaluation

**EAL 5 augmenté  
ALC\_DVS.2, AVA\_VAN.5**

Développeur

**SAMSUNG Electronics Co. Ltd**  
Chip Card & Microcontroller  
San#24 Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggi-Do, 449-711  
République de Corée

Commanditaire

**SAMSUNG Electronics Co. Ltd**  
Chip Card & Microcontroller  
San#24 Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggi-Do, 449-711  
République de Corée

Centre d'évaluation

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

Accords de reconnaissance applicables



**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](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 DES PRODUITS .....  | 6         |
| 1.2.1. <i>Identification du produit</i> .....  | 6         |
| 1.2.2. <i>Services de sécurité</i> .....   | 7         |
| 1.2.3. <i>Architecture</i> .....   | 7         |
| 1.2.4. <i>Cycle de vie</i> .....   | 9         |
| 1.2.5. <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 .....  | 13        |
| 3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....   | 13        |
| 3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....                        | 14        |
| <b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</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>17</b> |

# 1. Le produit

## 1.1. Présentation du produit

Les produits évalués sont les microcontrôleurs « SAMSUNG S3FV9QM/S3FV9QK, revision 3 » 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 des produits

La cible de sécurité [ST] définit les produits évalués, leurs fonctionnalités de sécurité évaluées et leurs environnements 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].

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

- microcontrôleur : **SAMSUNG S3FV9QM/S3FV9QK, revision 3** ;
- bibliothèques logicielles : *Test ROM v1.0, Boot loader v2.1, Crypto Library v1.1 ou v1.2, DTRNG library v2.0.*

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

- identification des microcontrôleurs :
  - o **0x1A16** pour S3FV9QM par lecture de deux octets à l'adresse 0x400004 ;
  - o **0x1A14** pour S3FV9QK par lecture de deux octets à l'adresse 0x400004 ;
- révision : **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* : **0x21** pour la révision 2.1 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* : **0x02** pour la révision 2 par lecture d'un octet à l'adresse 0x40002F ;

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, dont les logiciels embarqués, que ce soit en exécution ou lorsqu'ils sont stockés 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 révision 1.2) ;
- le support à la génération de nombres non prédictibles.

### 1.2.3. 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), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, ... ;
  - o de modules fonctionnels : gestion des entrées/sorties en mode contact (interfaces ISO 7816 et « *SWP*<sup>3</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 :
  - o en ROM, un logiciel de test du microcontrôleur inclus dans la cible d'évaluation.

---

<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> *Single Wire Protocol* ou protocole simple connexion.

L'architecture matérielle du microcontrôleur peut être représentée de la façon suivante :

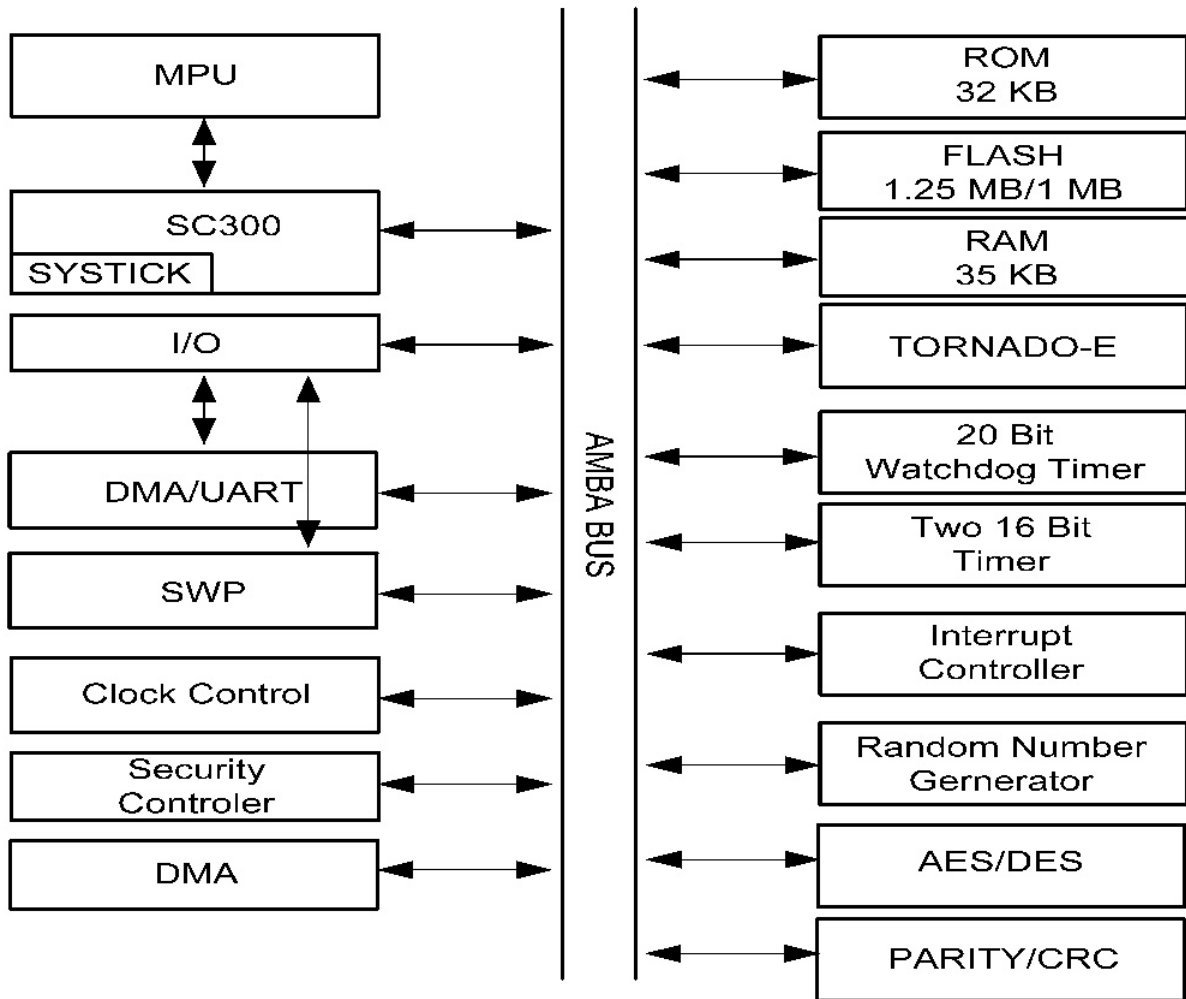


Figure 1: Architecture



### 1.2.4. Cycle de vie

Le cycle de vie des produits est le suivant :

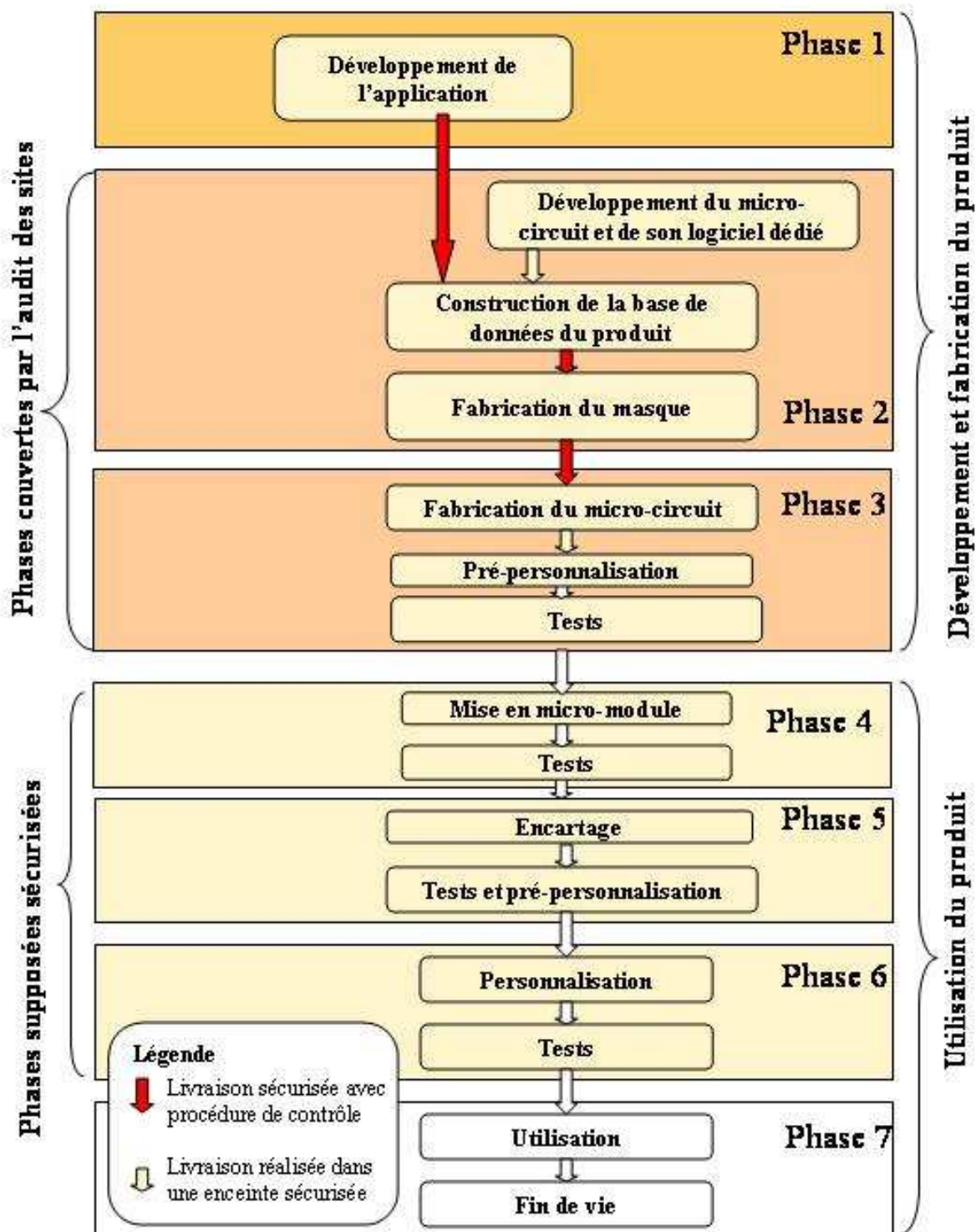


Figure 2: Cycle de vie

Au regard du cycle de vie, les produits sont évalués en sortie de la phase 3 du cycle de vie.

Les produits ont été développés sur les sites suivants :

- site de conception :

**Giheung Plant / SR3 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 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**

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 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 » : 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.

### **1.2.5. Configuration évaluée**

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et aux logiciels 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 donc les tests n'ont 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 3** [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 [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 17 janvier 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

Les produits comportent un générateur d'aléas de type DTRNG (« *Digital True Random Number Generator*<sup>1</sup> ») construit à partir d'un support matériel.

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS31] par le centre d'évaluation. Le générateur atteint le niveau P2.

Dans le cas où le DTRNG serait utilisé à des fins cryptographiques, il est obligatoire de le combiner (voir [GUIDES]) à un mécanisme algorithmique de génération de pseudo-aléa (retraitement cryptographique), afin de fournir des données aléatoires cryptographiquement satisfaisantes, comme énoncé dans les documents [REF].

---

<sup>1</sup> Générateur physique et numérique de nombres aléatoires.

## 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, revision 3 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans la 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, revision 3 » 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<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

| 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<br>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<br>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<br>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<br>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<br>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<br>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

|          |  |
|----------|--|
| [ST]     | Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none"> <li>- <i>Security Target of Samsung S3FV9QM/QK</i>, version 3.2, 26<sup>th</sup> september 2012, Samsung Electronics Co, Ltd.</li> <li>- <i>Security Target Lite of Samsung S3FV9QM/QK</i>, version 3.2, 17<sup>th</sup> january 2013, Samsung Electronics Co, Ltd.</li> </ul>   |
| [RTE]    | Rapport technique d'évaluation : <ul style="list-style-type: none"> <li>- <i>Evaluation Technical Report CAYUSE</i>, Ref. LETI.CESTI.CAY.RTE.001, 17<sup>th</sup> january 2013, v1.3, CEA-LETI.</li> <li>- <i>Evaluation Technical Report Lite CAYUSE</i>, Ref. LETI.CESTI.CAY.RT.002, 25<sup>th</sup> january 2013, v1.0, CEA-LETI.</li> </ul>  |
| [CONF]   | Liste de configuration du produit <ul style="list-style-type: none"> <li>- <i>Project &lt;CAYUSE&gt;Life Cycle Definition (Class ALC_CMC.4/CMS.5)</i>, version 3.3, 27<sup>th</sup> september 2012, SAMSUNG.</li> </ul>  |
| [GUIDES] | Guides du produit : <ul style="list-style-type: none"> <li>- <i>S3FV9QM/QK 32-Bit CMOS Microcontroler for SmartCard, User's Manual</i>, reference S3FV9QM_UM_REV1.03, rev 1.03, 24<sup>th</sup> september 2012, Samsung Electronics Co, Ltd ;</li> <li>- <i>Boot Loader Specification for S3FV9QM</i>, version 0.4, 19<sup>th</sup> september 2012, Samsung Electronics Co, Ltd ;</li> <li>- <i>TORNADO-E RSA Library API Manual</i>, reference TN_TorE_RSA_APIManual_v1.00a, version 1.00a, 9<sup>th</sup> january 2012, Samsung Electronics Co, Ltd ;</li> <li>- <i>TORNADO-E RSA/ECC Library API Manual</i>, reference TN_TorE_RSAECC_APIManual_v1.32a, version 1.32a, 31<sup>st</sup> august 2012, Samsung Electronics Co, Ltd ;</li> <li>- <i>S3FV9XX HW DTRNG and DTRNG library application note</i>, reference S3FV9XX_DTRNG_AN_v1.2, version 1.2, 26<sup>th</sup> april 2012, Samsung Electronics Co, Ltd ;</li> <li>- <i>Security Application Note S3FV9QM</i>, version 1.0, 24<sup>th</sup> april 2012, Samsung Electronics Co, Ltd ;</li> <li>- <i>S3FV9QM/QK Chip Delivery Specification</i>, revision 0.1, march 2012, Samsung Electronics Co, Ltd ;</li> </ul> |
| [PP0035] | <i>Protection Profile, Security IC Platform Protection Profile Version 1.0</i> June 2007. Certifié par le BSI ( <i>Bundesamt für Sicherheit in der Informationstechnik</i> ) 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 :<br>Part 1: Introduction and general model,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001;<br>Part 2: Security functional components,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002;<br>Part 3: Security assurance components,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003. |
| [CEM]      | Common Methodology for Information Technology Security Evaluation :<br>Evaluation Methodology,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.   |
| [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 2.8, January 2012.   |
| [COMP]     | Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.  |
| [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 <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a> .   |
| [AIS 31]   | Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).   |