



*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-2014/59**

# **Microcontrôleur SAMSUNG S3FT9PE Révision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4**

*Paris, le 14 août 2014*

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

Contre-amiral Dominique RIBAN  
[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.

|  |   |
|--|---|
| <i>Référence du rapport de certification</i> | <b>ANSSI-CC-2014/59</b>   |
| <i>Nom du produit</i>                        | <b>Microcontrôleur SAMSUNG S3FT9PE Révision 0<br/>embarquant la bibliothèque RSA/ECC optionnelle<br/>TORNADO 2MX2 v2.4</b>  |
| <i>Référence/version du produit</i>          | <b>Revision 0</b>   |
| <i>Conformité à un profil de protection</i>  | <b>[PP0035] : Security IC Platform Protection Profile<br/>Version 1.0</b>   |
| <i>Critères d'évaluation et version</i>      | <b>Critères Communs version 3.1 révision 4</b>  |
| <i>Niveau d'évaluation</i>                   | <b>EAL 5 augmenté<br/>ALC_DVS.2, AVA_VAN.5</b>  |
| <i>Développeur</i>                           | <b>Samsung Electronics Co. Ltd.<br/>17 Floor, B-Tower, 1-1, Samsungjeonja-ro<br/>Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud</b>   |
| <i>Commanditaire</i>                         | <b>Samsung Electronics Co. Ltd.<br/>17 Floor, B-Tower, 1-1, Samsungjeonja-ro<br/>Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud</b>   |
| <i>Centre d'évaluation</i>                   | <b>CEA - LETI<br/>17 rue des martyrs, 38054 Grenoble Cedex 9, France</b>  |
| <i>Accords de reconnaissance applicables</i> | <div style="display: flex; justify-content: space-around; align-items: center;"><div style="text-align: center;"><p><b>CCRA</b></p></div><div style="text-align: center;"><p><b>SOG-IS</b></p></div></div> <p><b>Le produit est reconnu au niveau EAL4.</b></p> |

## 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> .....   | 8         |
| 1.2.6. <i>Configuration évaluée</i> .....  | 9         |
| <b>2. L’EVALUATION .....</b>   | <b>11</b> |
| 2.1. REFERENTIELS D’EVALUATION .....   | 11        |
| 2.2. TRAVAUX D’EVALUATION .....  | 11        |
| 2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LE REFERENTIEL TECHNIQUE DE<br>L’ANSSI ..... | 11        |
| 2.4. ANALYSE DU GENERATEUR D’ALEAS .....   | 11        |
| <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 .....</b>  | <b>15</b> |
| <b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>                                | <b>17</b> |
| <b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>                                       | <b>19</b> |

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le « Microcontrôleur SAMSUNG S3FT9PE Révision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 » développé par Samsung Electronics Co. Ltd.

Le produit est physiquement identique à celui précédemment certifié sous la référence [ANSSI-CC-2013/46]. Les modifications portent sur :

- le DTRNG<sup>1</sup> (*Digital True Random Number Generator*) appelé ici DTRNG FRO, un générateur matériel déjà présent sur le produit mais ne faisant pas partie de la TOE (*Target Of Evaluation* – Cible d'évaluation) précédemment certifiée ;
- le code du *Bootloader* qui passe en version 4.5 ;
- l'ajout de deux sites au cycle de vie des produits (voir chapitre 1.2.5).

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, etc) 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]. Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire située à l'offset 0x400000 :

- identification des microcontrôleurs :
  - o 0x190E, désignant le modèle S3FT9PE, par lecture de deux octets à l'adresse 0x400004 ;

---

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

- révision :
  - o 0x00 pour la révision 0 par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :
  - o *Test ROM Code* : 0x10 pour la version 1.0 par lecture d'un octet à l'adresse 0x40002B ;
  - o *Secure Boot loader* : 0x45 pour la version 4.5 par lecture d'un octet à l'adresse 0x400030 ;

L'identification des bibliothèques se fait par des fonctions spécifiques :

- *RSA Library Version* : 0x322E34 pour la version 2.4 par lecture de la 14<sup>e</sup> à la 16<sup>e</sup> valeurs hexadécimales ASCII retournées par la fonction *RSA\_library\_version\_info* ;
- *ECC Library Version* : 0x322E34 pour la version 2.4 par lecture de la 13<sup>e</sup> à la 15<sup>e</sup> valeurs hexadécimales ASCII retournées par la fonction *EC\_library\_version\_info* ;
- *DTRNG Library Version* : 0x0600 pour la version 6.0 par lecture de la 1<sup>er</sup> et de la 2<sup>de</sup> valeurs hexadécimales retournées par la fonction *DTRNG\_version*.

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 et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support à la génération de nombres non prédictibles.

### 1.2.4. Architecture

Le microcontrôleur S3FT9PE est constitué des éléments suivants :

- une partie matérielle comprenant :
  - o un processeur SecuCalm RISC 16 bits ;
  - o des mémoires :
    - 36 Ko de ROM dont 4 Ko occupés par les logiciels de test embarqués (*Test ROM Code*) ;
    - 4 Ko de RAM ;
    - 200 Ko de FLASH ;
  - 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, etc ;
  - o des modules fonctionnels : gestion des entrées/sorties en mode contact (UART ISO 7816), génération de nombres aléatoires – DTRNG (*Digital True Random Number Generator*), coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO 2MX2 ;
- une partie logicielle composée :
  - o des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
  - o d'une bibliothèque pour le DTRNG ;

- de la bibliothèque de calcul arithmétique pour la cryptographie asymétrique *TORNADO 2MX2 Secure RSA/ECC library*, version 2.4 ; cette bibliothèque est optionnelle et peut être désactivée avant la livraison du microcontrôleur ;
- d'un *Secure Boot Loader* (utilisant le coprocesseur DES) 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 :

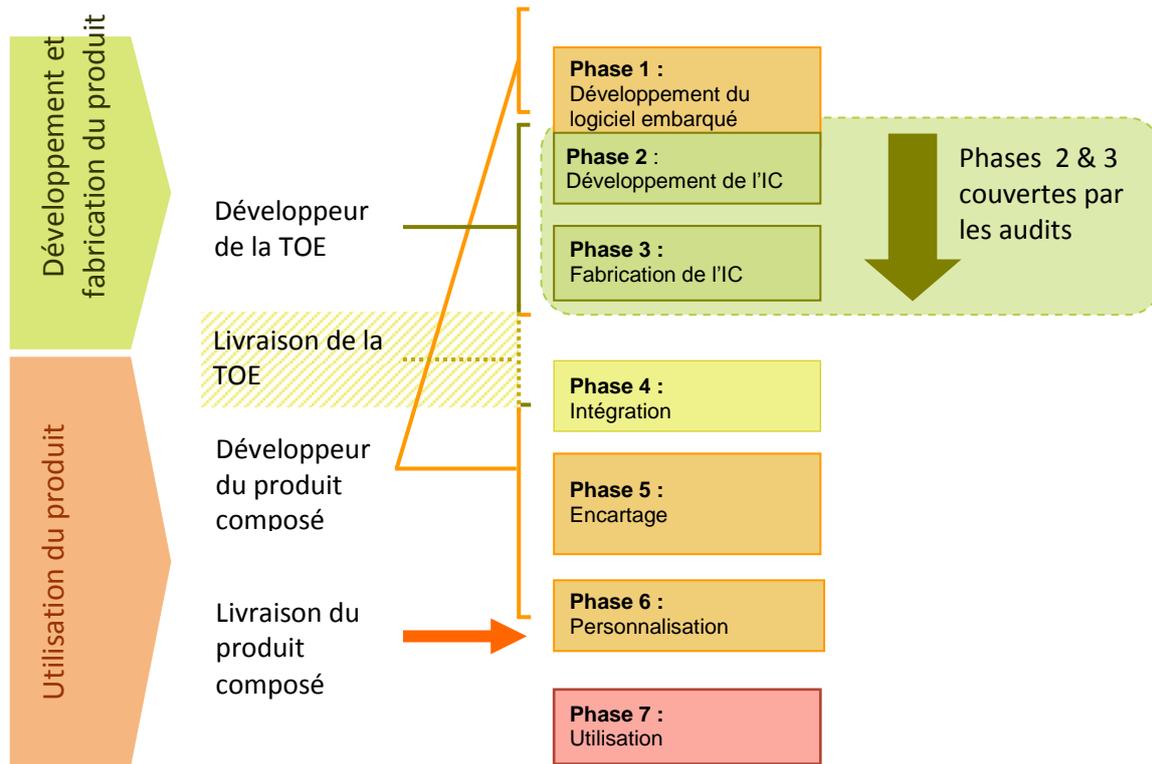


Figure 1 : Cycle de vie du produit

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.

La phase 2 correspond à la phase de développement du microcontrôleur et comprend notamment les étapes suivantes :

- conception du circuit ;
- développement du logiciel dédié.

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

- intégration et fabrication du masque ;
- fabrication du circuit ;
- test du circuit ;
- préparation ;
- pré-personnalisation si nécessaire.

La TOE est développée sur les sites suivants :

**Giheung Plant (Phase 2 & 3)**

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

**HANAMICRON Plant (Phase 3)**

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

**Hwasung Plant (Phase 3)**

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

**Eternal Plant (Phase 3)**

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

**PKL Plant (Phase 3)**

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

**ChangFeng Plant (Phase 3)**

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

**TESNA Plant**

No. 450-2 Mogok-Dong,  
Pyeongtaek-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* » ;
- configuration « *NORMAL mode* », qui supporte deux sous-modes d'exécution pour le processeur :
  - o 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* » ;
  - o le sous-mode « *USER* » : mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible.

**1.2.6. Configuration évaluée**

Le certificat porte sur le microcontrôleur et les bibliothèques logicielles qu'il embarque tels que définis au chapitre 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.

## 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

L'évaluation s'appuie sur les résultats d'évaluation du Microcontrôleur SAMSUNG S3FT9PE Révision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 certifiés le 2 juillet 2013 sous la référence [ANSSI-CC-2013/46].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18 avril 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 le référentiel technique 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 DTRNG, appelé DTRNG FRO, incluant un retraitement qui a fait l'objet d'une analyse par le CESTI (voir [ANSSI-CC-2014/37]). Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des nombres générés. 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* ».

Les guides associés au générateur d'aléas, 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 S3FT9PE Révision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 » 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 S3FT9PE Révision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le microcircuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES]. Les recommandations du chapitre « 2.4. Analyse du générateur d'aléas » devront également être suivies.

### 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   | Security architecture description   |
|   | ADV_FSP | 1                                 | 2     | 3     | 4     | 5     | 5     | 6     | 5   | Complete semi-formal functional specification with additional error information |
|   | ADV_IMP |                                   |       |       | 1     | 1     | 2     | 2     | 1   | Implementation representation of the TSF  |
|   | ADV_INT |                                   |       |       |       | 2     | 3     | 3     | 2   | Well-structured internals   |
|   | ADV_SPM |                                   |       |       |       |       | 1     | 1     |   |   |
|   | ADV_TDS |                                   | 1     | 2     | 3     | 4     | 5     | 6     | 4   | Semi-formal modular design  |
| AGD<br>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<br>Support au cycle de vie            | ALC_CMC | 1                                 | 2     | 3     | 4     | 4     | 5     | 5     | 4   | Production support, acceptance procedures and automation                        |
|   | ALC_CMS | 1                                 | 2     | 3     | 4     | 5     | 5     | 5     | 5   | Development tools CM coverage   |
|   | ALC_DEL |                                   | 1     | 1     | 1     | 1     | 1     | 1     | 1   | Delivery procedures   |
|   | ALC_DVS |                                   |       | 1     | 1     | 1     | 2     | 2     | 2   | Sufficiency of security measures  |
|   | ALC_LCD |                                   |       | 1     | 1     | 1     | 1     | 2     | 1   | Developer defined life-cycle model  |
|   | ALC_TAT |                                   |       |       | 1     | 2     | 3     | 3     | 2   | Compliance with implementation standards  |
| ASE<br>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<br>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   |

|  |         |   |   |   |   |   |   |   |   |   |
|--|---------|---|---|---|---|---|---|---|---|---|
| <b>AVA</b><br><b>Estimation des</b><br><b>vulnérabilités</b> | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 5 | Advanced methodical<br>vulnerability analysis |
|--|---------|---|---|---|---|---|---|---|---|---|

## Annexe 2. Références documentaires du produit évalué

|          |  |
|----------|--|
| [ST]     | <p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"><li>- <i>Security Target of S3FT9PE 16-Bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software</i>, version 3.1, 14 avril 2014, Samsung.</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>- <i>Security Target Lite of Samsung S3FT9PE 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software</i>, version 2.2, 15 avril 2014, Samsung.</li></ul>              |
| [RTE]    | <p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"><li>- <i>Evaluation Technical Report</i>, Référence LETI.CESTI.KLA3R.ANSSI.001 - v1.0, 18 avril 2014, CEA-LETI.</li></ul>  |
| [CONF]   | <p>Liste de configuration du produit :</p> <ul style="list-style-type: none"><li>- <i>Project &lt; KLALLAM3R &gt; Life Cycle Definition (Class ALC_CMC.4/CMS.5)</i>, version 1.7, 18 avril 2014, Samsung.</li></ul>  |
| [GUIDES] | <p>Guides du produit :</p> <ul style="list-style-type: none"><li>- <i>Security Application Note for S3FT9FD/FC/FB, PF/PT/PS, PE, FA</i>, 13 mars 2014, version 1.6, Samsung ;</li><li>- <i>S3FT9PF / T9PT / T9PS Chip Delivery Specification</i>, mars 2014, version 1.2, Samsung ;</li><li>- <i>S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note</i>, 20 novembre 2013, version 1.4, Samsung ;</li><li>- <i>TORNADO-2Mx2 RSA/ECC Library API Manual</i>, 07 février 2014, version 2.23, Samsung ;</li><li>- <i>SecuCalm CPU CORE, architecture reference</i>, 3 mars 2011, version AR14, Samsung ;</li><li>- <i>Bootloader User's Manual for S3FT9xx Family Products</i>, 8 avril 2013, version 1.5, Samsung ;</li></ul> |

|                    |   |
|--------------------|---|
|                    | <ul style="list-style-type: none"> <li>- <i>Bootloader User's Manual Guide errata</i>, 7 mars 2014, version 5.0, Samsung ;</li> <li>- <i>S3FT9XX 16 bit CMOS Microcontroller for Smart Card User's Manual</i>, 30 septembre 2013 , version 1.10, Samsung ;</li> <li>- <i>User's Manual errata</i>, février 2014, version 0.5, Samsung.</li> </ul> |
| [PP0035]           | Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI sous la référence BSI-PP-0035-2007.</i>   |
| [ANSSI-CC-2013/46] | « Microcontrôleur SAMSUNG S3FT9PE Révision 0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.4 »<br><i>Certifié le 2 juillet 2013 sous la référence ANSSI-CC-2013/46.</i>  |
| [ANSSI-CC-2014/37] | « Microcontrôleurs SAMSUNG S3FT9MD et S3FT9MC Révision 0 »<br><i>Certifié le 11 juillet 2014 sous la référence ANSSI-CC-2014/37.</i>  |

### 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>September 2012, version 3.1, revision 4, ref CCMB-2012-09-001;<br>Part 2: Security functional components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-002;<br>Part 3: Security assurance components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-003. |
| [CEM]  | Common Methodology for Information Technology Security Evaluation :<br>Evaluation Methodology,<br>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, February 2009.   |
| [JIWG AP]*   | Mandatory Technical Document – Application of attack potential to smart-cards, JIWG, version 2.9, January 2013.  |
| [CC RA]  | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.  |
| [SOG-IS]   | « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.  |
| [REF]  | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .   |
| [AIS 31]   | <i>Functionality classes and evaluation methodology for physical random number generator</i> , AIS31 version 1, 25 September 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.