



*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-2016/65**

### **S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure/CM1 RSA and ECC Library including specific IC Dedicated Software**

*Paris, le 14 octobre 2016*

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

Guillaume POUPARD  
[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@ssi.gouv.fr](mailto:certification@ssi.gouv.fr)

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

Référence du rapport de certification

**ANSSI-CC-2016/65**

Nom du produit

**S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for  
Smart Card with optional Secure/CM1 RSA and ECC Library  
including specific IC Dedicated Software**

Référence/version du produit

**S3FT9MF/S3FT9MT/S3FT9MS\_rev1-2\_SW10-50-60-20-24-102\_20\_GU111-15\_12-21-225-10\_20-19-19-14-20-06**

Conformité à un profil de protection

**Security IC Platform Protection Profile  
with Augmentation Packages, version 1.0,  
certifié BSI-CC-PP-0084-2014 le 19 février 2014**

avec conformité à

**“Package 1: Loader dedicated for usage in Secured Environment only”  
“Package 2: Loader dedicated for usage by authorized users only”**

Critères d'évaluation et version

**Critères Communs version 3.1 révision 4**

Niveau d'évaluation

**EAL 6 augmenté  
ASE TSS.2**

Développeurs

**Samsung Electronics Co. Ltd.**  
17 Floor, B-Tower, 1-1, Samsungjeonja-ro  
Hwaseong-si, Gyeonggi-do  
445-330 Corée du Sud

**Trusted Labs**  
5, rue du Baillage  
78000 Versailles,  
France

Commanditaire

**Samsung Electronics Co. Ltd.**  
17 Floor, B-Tower, 1-1, Samsungjeonja-ro  
Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud

Centre d'évaluation

**CEA - LETI**

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables



**Le produit est reconnu au niveau EAL2.**

## Préface

### La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet [www.ssi.gouv.fr](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. Introduction .....	6
1.2.2. Identification du produit .....	6
1.2.3. Services de sécurité .....	7
1.2.4. Architecture .....	7
1.2.5. Cycle de vie .....	8
1.2.6. Configuration évaluée .....	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>14</b>
3.1. CONCLUSION .....	14
3.2. RESTRICTIONS D’USAGE .....	14
3.3. RECONNAISSANCE DU CERTIFICAT .....	15
3.3.1. Reconnaissance européenne (SOG-IS) .....	15
3.3.2. Reconnaissance internationale critères communs (CCRA) .....	15
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT .....</b>	<b>16</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 « S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure/CM1 RSA and ECC Library including specific IC Dedicated Software » de référence S3FT9MF/S3FT9MT/S3FT9MS\_rev1-2\_SW10-50-60-20-24-102\_20\_GU111-15\_12-21-225-10\_20-19-19-14-20-06, développé par *SAMSUNG ELECTRONICS CO. LTD* et *TRUSTED LABS*.

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 [PP0084], avec les packages « *Loader dedicated for usage in secured environment only* » et « *Loader dedicated for usage by authorized users only* ».

### 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 0x160F, 0x161D et 0x161C désignant respectivement les modèles S3FT9MF, S3FT9MT et S3FT9MS, par lecture de deux octets à l'adresse 0x400004 ;
- révision :
  - o 0x01 (respectivement 0x02) pour la révision 1 (respectivement révision 2) 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* : 0x50 pour la version 5.0 par lecture d'un octet à l'adresse 0x400030.

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

- *TORNADO 2Mx2 Secure RSA/ECC library* : "S3CT9XX RSA v2.4" (codage ASCII) par appel à la fonction *RSA\_library\_version\_info* et "S3CT9XX EC v2.4" par appel à la fonction *EC\_library\_version\_info* ;
- *TORNADO 2Mx2 CM1 Secure RSA/ECC library* : "PKA\_Lib\_CM1\_v1.02" ou "PKA\_Lib\_CM1\_v2.00" par appel à la fonction *PKA\_library\_version\_info* ;
- *DTRNG FRO Library* : 0x0600 pour la version 6.0 par lecture des 1<sup>ère</sup> et 2<sup>de</sup> valeurs hexadécimales retournées par la fonction *DTRNG\_version* ;
- *EHP DTRNG FRO Library* : 0x0200 pour la version 2.0 par lecture des 1<sup>ère</sup> et 2<sup>de</sup> valeurs hexadécimales retournées par la fonction *DTRNG\_version*.

Cette procédure d'identification est introduite dans le guide « *Chip Delivery Specification* » (voir [GUIDES]).

### 1.2.3. Services de sécurité

Les principaux services de sécurité fournis par les produits 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 ou asymétriques ;
- le support à la génération de nombres non prédictibles.

### 1.2.4. Architecture

Les produits sont constitués des éléments suivants :

- une partie matérielle comprenant :
    - o un processeur SecuCalm RISC 16 bits ;
    - o des mémoires :
      - 32 Ko de ROM dont 4 Ko occupés par les logiciels de test embarqués (*Test ROM Code*) ;
      - 6,5 Ko de RAM dont 2.5Ko dédiés au coprocesseur arithmétique ;
      - 264, 232 et 212 Ko de FLASH respectivement pour les modèles S3FT9MF, S3FT9MT et S3FT9MS ;
    - 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*<sup>1</sup>) et BPRNG (*Bilateral Pseudo-Random Number Generator*) à usage interne uniquement, coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO 2MX2 ;
- La version 1 et la version 2 de la partie matérielle présentent des différences dans la gestion de l'alimentation, la version 2 permettant une communication sans-contact lorsque le microcontrôleur est alimenté en contact ;
- 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 ;

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

- de bibliothèques pour la génération de nombres aléatoires *DTRNG FRO library*, version 6.0 et *EHP DTRNG FRO library*, version 2.0 ;
- de bibliothèques pour la cryptographie asymétrique *TORNADO 2Mx2 Secure RSA/ECC library*, version 2.4 et *TORNADO 2Mx2 CM1 Secure RSA/ECC library*, version 1.02 ou version 2.00 ; ces bibliothèques sont optionnelles et peuvent être désactivées ou absentes lors de la livraison du microcontrôleur ;
- d'un *Secure Boot Loader*, version 5.0, 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 :

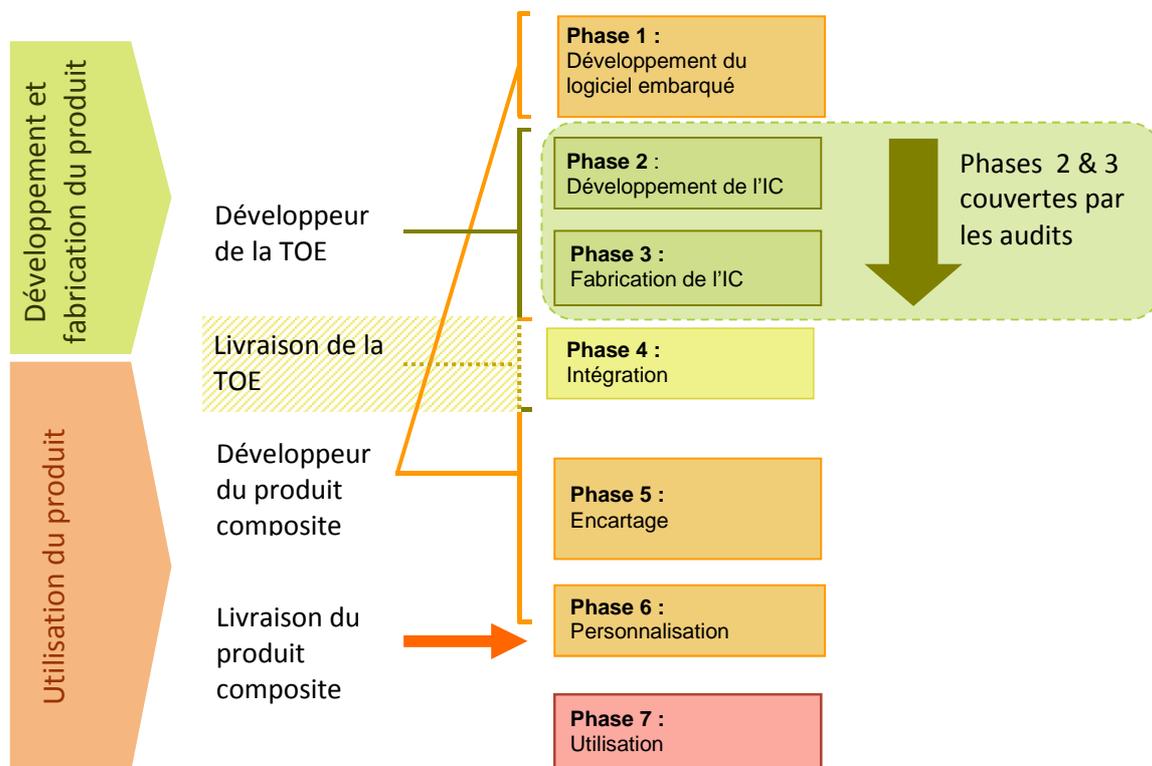


Figure 1 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de *wafers*. En option, la TOE peut également être livrée intégrée en boîtiers après la 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 :

Nom du Site	Adresse	Fonction
<i>TRUSTED LABS</i>	<i>TRUSTED LABS</i> 5, rue du Baillage 78000 Versailles France	Phase 2 : fournitures spécifiques pour ADV_SPM.1 et ADV_INT.3 Co-édition de la Cible de Sécurité
<i>HWASUNG PLANT/DSR BUILDING</i>	1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, Corée du Sud San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 2 : <i>Smart Card Design Center</i>
<i>HWASUNG PLANT/DSR BUILDING</i>		Phase 3 : <i>Test program development</i>
<i>HWASUNG PLANT/NRD BUILDING</i>		Phase 3 : <i>Mask Shop</i>
<i>PKL PLANT</i>	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : <i>Mask Shop</i>
<i>GIHEUNG PLANT/LCD BUILDING</i>	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 446-711 Corée du Sud	Phase 3 : <i>Mask Fabrication Line</i>
<i>GIHEUNG PLANT/LINE 6,S1</i>		Phase 3 : <i>IC Fabrication</i>
<i>GIHEUNG PLANT/LINE 2</i>		Phase 3 : <i>Testing, Wafer Stock, Inking, Back Side Grinding</i>
<i>HANAMICRON PLANT</i>	95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : <i>Backlap, Sawing</i>
<i>TESNA PLANT</i>	450-2 Mogok-Dong, Pyeungtaek City, Gyeonggi, Corée du Sud	Phase 3 : <i>Testing</i>
<i>ASE KOREA</i>	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : <i>Backlap, Sawing, SIP module assembly</i>
<i>ETERNAL PLANT</i>	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 3&4 : <i>Sawing, COB</i>
<i>INESA PLANT</i>	No. 818 Jin Yu Road Jin Qiao Export Processing Zone Pudong, Shanghai, Chine	Phase 3&4 : <i>Backlap, Sawing, COB</i>
		Phase 4 : <i>Packaging, Warehouse</i>
<i>ONYANG PLANT</i>	San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 4 : <i>Wafer Stock, Packaging, Package Testing, Warehouse</i>
<i>ETERNAL PLANT</i>	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 4 : <i>Packaging, Warehouse</i>

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 « *PRIVILEGE* », activé lors de l'exécution de routines d'interruption, est un mode d'exécution interne au processeur qui permet d'accéder aux registres de contrôle et de sécurité et de configurer la MPU (*Memory Protection Unit*) ; lorsque le processeur a terminé l'exécution de la routine, il retourne automatiquement en mode « *USER* » ;
  - le sous-mode « *USER* » : mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible.

### ***1.2.6. Configuration évaluée***

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au 1.2.1. 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 1.2.4, le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de *wafer*, ou à l'issue de la phase 4 lorsque le produit est livré en boîtiers (micro-modules, etc.).

## 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 « Microcontrôleurs Samsung S3FT9MF/S3FT9MT/S3FT9MS avec bibliothèques optionnelles RSA et ECC » certifié le 18 janvier 2016 sous la référence [ANSSI-CC-2016/01]. Les principales différences avec le produit précédemment certifié sont :

- au niveau logiciel, la possibilité d'utiliser de nouvelles versions de la librairie cryptographique *CM1 Secure RSA/ECC library* ;
- au niveau des guides, l'amélioration de contremesures à appliquer, afin de prendre en compte l'état de l'art du potentiel d'attaques visé.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 août 2016, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

### 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA\_VAN.5 visé.

### 2.4. Analyse du générateur d'aléas

Le produit embarque un générateur physique d'aléa qui a fait l'objet d'une analyse par le CESTI, appelé DTRNG FRO, incluant un retraitement de lissage, et utilisable à travers une bibliothèque fournie par le développeur. Les règles RègleArchiGVA-1 et RègleArchiGVA-2 ainsi que la recommandation RecomArchiGVA-1 de [REF] s'avèrent respectées.

Le document [REF] impose, pour un usage cryptographique, que la sortie d'un générateur matériel de nombres aléatoires subisse un retraitement algorithmique de nature

cryptographique ; ce retraitement n'est pas implémenté dans le produit et devra être développé par l'utilisateur le cas échéant, comme indiqué dans « *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note* » (voir [GUIDES]).

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

Les guides associés au générateur d'aléa, notamment : « *S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note* » et « *Security Application Note for S3FT9MD/MC, MF/MT/MS, MH/MV/MG* » (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 « S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure/CM1 RSA and ECC Library including specific IC Dedicated Software » de référence S3FT9MF/S3FT9MT/S3FT9MS\_rev1-2\_SW10-50-60-20-24-102\_20\_GU111-15\_12-21-225-10\_20-19-19-14-20-06 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL6 augmenté du composant ASE\_TSS.2.

### 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 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 lorsque les dépendances CC sont satisfaites. 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 EAL2 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, le Qatar, 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, EAL							Niveau d'assurance retenu pour le produit		
		1	2	3	4	5	6	7	6+	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	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	3	Minimally complex internals
	ADV_SPM						1	1	1	1	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	5	5	Complete 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	5	5	Advanced support
	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	3	3	Compliance with implementation standards - all parts
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	2	2	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		1	2	2	2	3	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	2	Ordered 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

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"><li>- S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure/CM1 RSA and ECC Library including specific IC Dedicated Software, ST (Security Target, version 9.4, 26 juillet 2016, 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>- S3FT9MF/S3FT9MT/S3FT9MS 16-bit RISC Microcontroller for Smart Card with optional Secure/CM1 RSA and ECC Library including specific IC Dedicated Software, ST (Security Target) Lite, version 9.1, 27 juillet 2016, Samsung.</li></ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"><li>- Evaluation Technical Report (full ETR) - LETI.CESTI.KLA5R5.FULL.001, version 1.1, 3 août 2016, 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 for Composition, LETI.CESTI.KLA5R5.COMPO.001, version 1.1, 4 août 2016, CEA-LETI.</li></ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"><li>- KLALLAM5R5, Life Cycle Definition (Class ALC_CMC.5/CMS.5), version 9.1, 27 juillet 2016, Samsung.</li></ul>

[GUIDES]	<p>Guides du produit :</p> <ul style="list-style-type: none"> <li>- S3FT9XX HW DTRNG FRO and DTRNG FRO Library Application Note, version 1.11, 10 juin 2015, Samsung ;</li> <li>- S3FT9XX HW DTRNG FRO and EHP DTRNG FRO Library Application Note, revision 1.5, 30 septembre 2015, Samsung ;</li> <li>- S3FT9XX, 16-bit CMOS Microcontroller for Smart Card, User's Manual, révision 1.20, septembre 2014, Samsung ;</li> <li>- Security Application Note for S3FT9MD/MC,MF/MT/MS, MH/MV/MG, version 2.1, 29 juin 2016, Samsung ;</li> <li>- Technical Report : TORNADO-2Mx2 RSA/ECC Library API Manual, TN_T2Mx2_RSAECC_APIManual_v2.25, version 2.25, 4 octobre 2014, Samsung ;</li> <li>- PKA Library API Manual, PKA_Lib_CM1_APIManual_v1.0, version 1.0, 18 décembre 2014, Samsung ;</li> <li>- RSA/ECC Library API Manual, CM1 RSA ECC Library API Manual v2.00, version 2.0, 22 février 2016, Samsung ;</li> <li>- S3FT9MF / T9MT / T9MS Chip Delivery Specification, version 1.9, juillet 2016, Samsung ;</li> <li>- Bootloader User's Manual for S3FT9xx Family Products, version 1.9, 9 juin 2015, Samsung ;</li> <li>- SecuCalm CPU CORE, Architecture Reference, référence: S3xT9xx_AR14_SecuCalmCore, version AR14, Samsung ;</li> <li>- 80nm FSID Devices Bootloader Specification Appendix, revision 2.0, juin 2015, Samsung;</li> <li>- (S3FT9XX_UM_REV1.20) User's Manual errata, version 0.60, octobre 2015.</li> </ul>
[PP0084]	<p>Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0084-2014 le 19 février 2014.</i></p>
[ANSSI-CC-2016/01]	<p>Rapport de certification ANSSI-CC-2016/01, Microcontrôleurs Samsung S3FT9MF/S3FT9MT/S3FT9MS avec bibliothèques optionnelles RSA et ECC, 18 janvier 2016, ANSSI.</p>

### Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[AIS 31]	Functionality classes and evaluation methodology for physical random number generator, AIS31, version 1, 25 septembre 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).

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