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-2012/27

SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 0

Paris, le 14 juin 2012

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

[ORIGINAL SIGNE]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2012/27

Nom et version du produit

SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 0

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, Giheug-gu, Yongin-City, Gyeonggi-Do, 449-771

République de Corée

Commanditaire

SAMSUNG Electronics Co. Ltd

Chip Card & Microcontroller

San#24 Nongseo-dong, Giheug-gu, Yongin-City, Gyeonggi-Do, 449-771

République de Corée

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

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.

Table des matières

1. Le produit

1.1. Présentation du produit

Les produits évalués sont les microcontrôleurs « SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 0 » développés par Samsung Electronics Co, Ltd.

La seule différence entre les produits S3FT9KF, S3FT9KT et S3FT9KS réside dans la taille de la mémoire FLASH : 264 Ko pour S3FT9KF, 232 Ko pour S3FT9KT et 212 Ko pour S3FT9KS.

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 S3FT9KF/S3FT9KT/S3FT9KS, *Revision* 0** ;
- librairies logicielles : *Test ROM v1.0, Secure Boot loader v0.0, TORNADO^{TM}2MX2Secure RSA/ECC Library v3.0 (option library), DRNG library v1, TRNG library v1* et *DTRNG library v1*.

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

- identification des microcontrôleurs :
  - **0x140F** pour S3FT9KF par lecture de deux octets à l'adresse 0x400004 ;
  - **0x141D** pour S3FT9KT par lecture de deux octets à l'adresse 0x400004 ;
  - **0x141C** pour S3FT9KS par lecture de deux octets à l'adresse 0x400004.
- révision : **0x00** pour la révision 0 par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :
  - *Test ROM* : **0x10** pour la révision 1.0 par lecture d'un octet à l'adresse 0x40002B ;
  - *Secure Boot loader* : **0x00** pour la révision 0.0 par lecture d'un octet à l'adresse 0x400030 ;
  - *TORNADO^{TM}2MX2Secure RSA/ECC Library (option library)* : **0x030C** pour la révision 3.0 par lecture de deux octets à l'adresse 0x40002C ;
  - *DRNG library* : **0x01** pour la révision 1 par lecture d'un octet à l'adresse 0x40002E ;

- *DTRNG/TRNG library* : **0x11** (DTRNG version 1, TRNG version 1) 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[1] ;
- la bonne exécution de services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles.

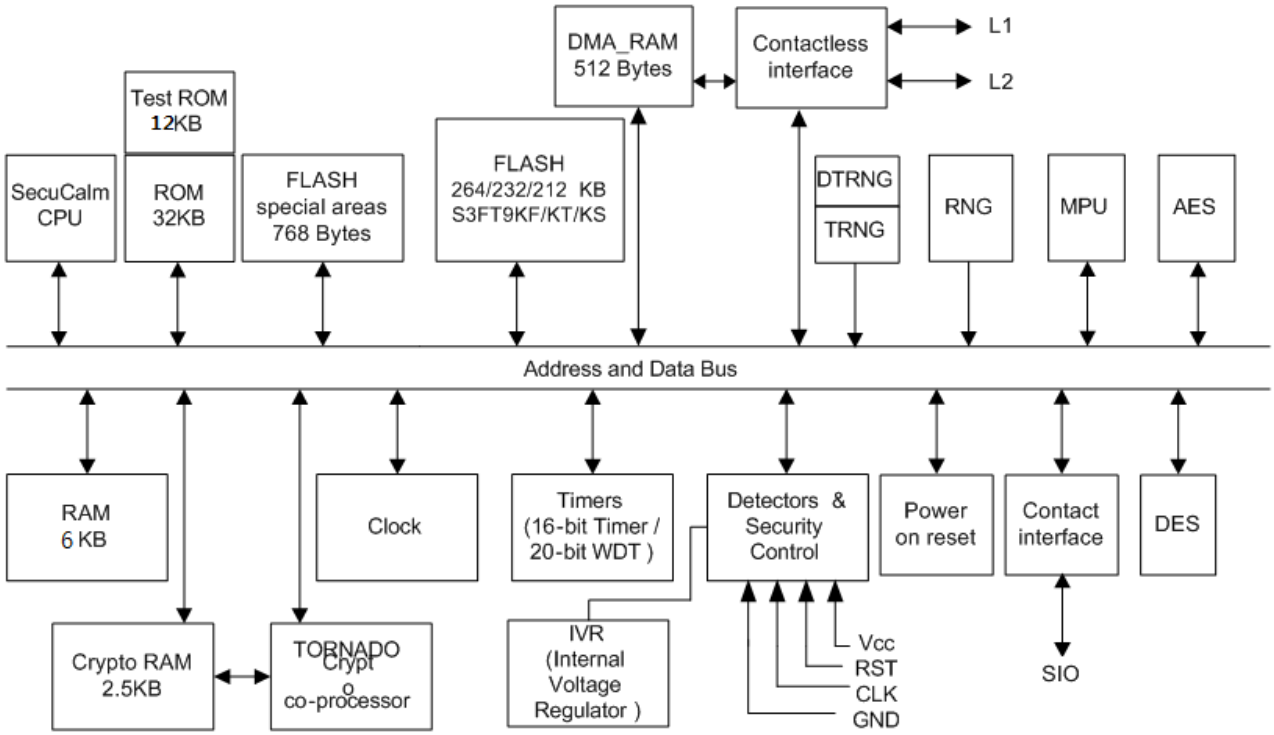
1.2.3. Architecture

Les microcontrôleurs S3FT9KF, S3FT9KT et S3FT9KS sont constitués des éléments suivants :

- une partie matérielle composée en particulier :
  - d'un processeur *16-bit CalmRISC CPU* ;
  - de mémoires :
    - FLASH dont 768 octets de mémoire spéciale et
      - 264 Ko pour le S3FT9KF ;
      - 232 Ko pour le S3FT9KT ;
      - 212 Ko pour le S3FT9KS.
    - 44 Ko de mémoire ROM dont 32 Ko pour le stockage des programmes utilisateurs et 12 Ko pour le Test ROM ;
    - 8.5 Ko de mémoire RAM dont 2.5 Ko spécifiques pour le calcul cryptographique ;
    - 512 octets de mémoire DMA RAM ;
  - 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,… ;
  - de modules fonctionnels : gestion des entrées/sorties en mode contact (IART ISO 7816) et sans contact (ISO 14443 type A et B), générateurs de nombres aléatoires – DRNG, TRNG et DTRNG –, crypto-processeurs 3DES et AES ainsi qu'un accélérateur cryptographique TORNADO^{TM}2MX2 pour le support d'algorithmes cryptographiques.
- une partie logicielle comprenant :
  - en ROM et en FLASH, des logiciels de test du microcontrôleur. Ces logiciels sont embarqués et font partie de la cible d'évaluation (TOE).

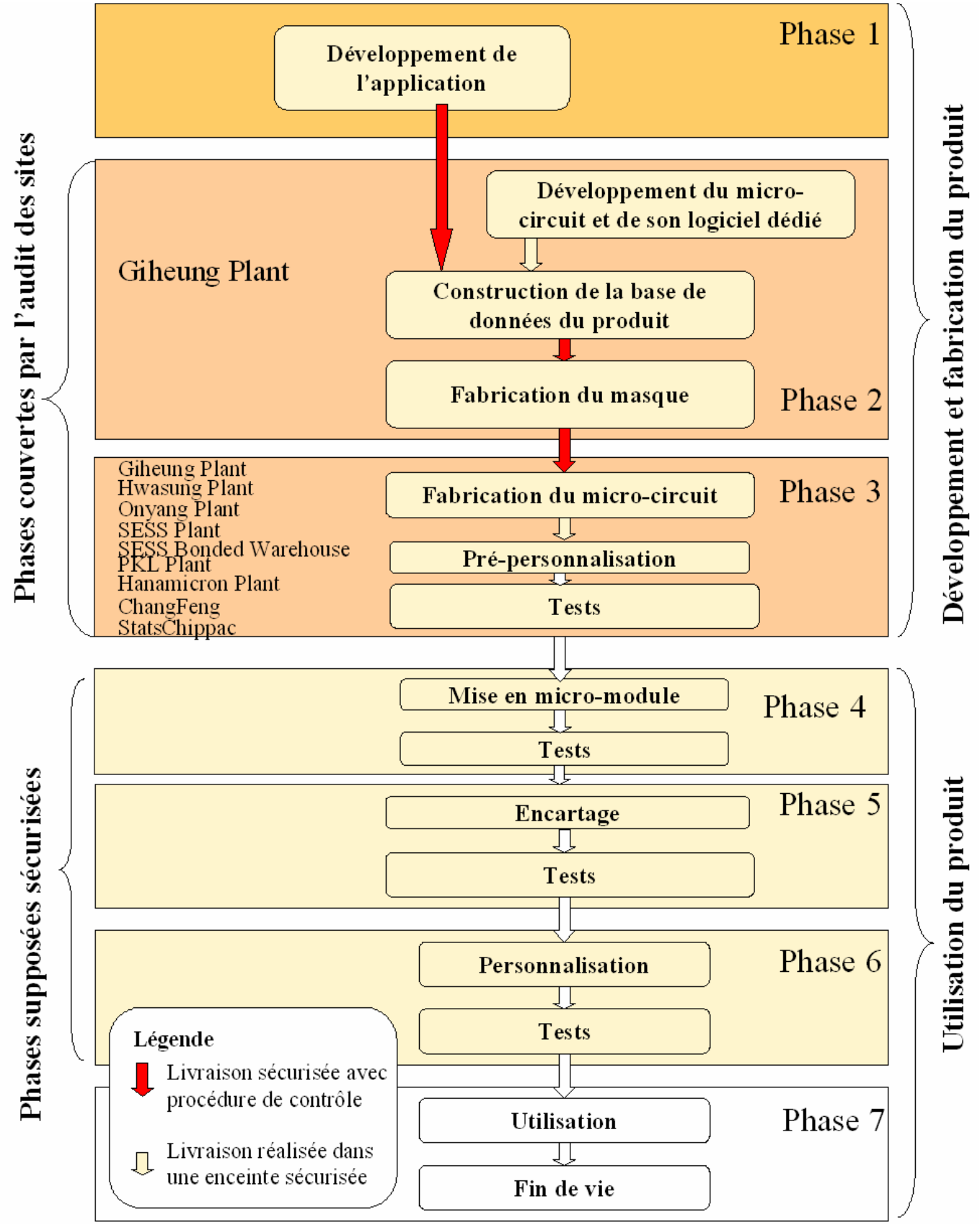
[1] *Target Of Evaluation* ou cible d'évaluation.

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



1.2.4. Cycle de vie

Le cycle de vie des produits est le suivant :



Les produits ont été développés sur les sites suivants :

- pour ce qui concerne la conception :

Giheung Plant

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

Giheung Plant

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

- pour ce qui concerne la fabrication des *wafers* :

Giheung Plant

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

Onyang-Plant

San #74, Buksoo-Ri, Baebang-Myun
Asan-City, Choongcheongnam-Do
République de Corée

- pour ce qui concerne le reste de la fabrication :

Giheung Plant

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

Hwasung Plant

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

Onyang-Plant

San #74, Buksoo-Ri, Baebang-Myun
Asan-City, Choongcheongnam-Do

République de Corée

SESS-Plant

No 15, Jin Ji Hu Road, Suzhou Industrial Park
Suzhou
République Populaire de Chine

SESS-Bonded Warehouse

No 88, morden road, Suzhou Industrial Park
Suzhou
République Populaire de Chine

PKL Plant

493-3, Sungsung-Dong,
Cheonan-City
Choongcheongnam-Do

République de Corée

Hanamicron Plant

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

ChangFeng Plant

No 818 Jin Yu Road,
Jin Qiao Export Processing Zone Pudong
Shangai

République Populaire de Chine

StatsChippac Plant

188 Huaxu Road,
Qingpu District
201702
Shangai
République Populaire de Chine

- pour ce qui concerne les tests :

Giheung Plant

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

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 :
  - mode « privilégié » : sous-ensemble du mode « *Normal mode* », réservé principalement au fonctionnement interne du microcontrôleur ;
  - 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.
Au regard du cycle de vie, le produit évalué est le produit qui sort de la phase 3 du cycle de vie.
Pour les besoins de l'évaluation, le produit fourni au centre d'évaluation est le microcontrôleur S3FT9KF, version 0 contenant les applications décrites au 1.2.1 (Test ROM version 1.0, Secure Boot loader révision 0.0, librairies DRNG et TRNG révision 1, librairie cryptographique TORNADO^{TM}2MX2Secure RSA/ECC révision 3.0). Le CESTI a jugé que le microcontrôleur S3FT9KF, version 0, était représentatif des trois produits qui font l'objet de ce rapport de certification.

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].

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.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 juin 2012, 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 trois générateurs d'aléas :

- un générateur d'aléas DRNG (*Digital Random Number Generator*[1]) construit à partir d'un support matériel et d'une librairie logicielle (post-traitement) ;
- un générateur TRNG (*True Random Number Generator*[2]) construit à partir d'un support matériel (source) ;
- un générateur DTRNG (*Digital True Random Number Generator*[3]) construit à partir d'un support matériel.

Ces trois générateurs d'aléas ont été évalués par le CESTI.
L'analyse conduite sur le DRNG n'a pas mis en évidence de biais statistiques bloquants pour un usage direct des sorties du générateur.
Dans le cas où le TRNG ou le DTRNG serait utilisé à des fins cryptographiques, il est obligatoire de le combiner 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].
Enfin, durant l'évaluation, le générateur DTRNG a été évalué selon la méthodologie [AIS31] (cas *alternative criteria for P2.d)(vii)*) par le CESTI. Il en ressort que le générateur est de classe P2 selon [AIS31].

[1] Générateur numérique de nombres aléatoires.
[2] Générateur physique de nombres aléatoires dit générateur « vrai ».
[3] Générateur physique et numérique de nombres aléatoires.

Les guides associés aux différents générateurs : « *Application Note DRNG Software Library v1.0 S3FT9Kx family* », « *S3FT9KX HW TRNG and AIS31 online test library application note* » et « *S3FT9KX HW DTRNG and DTRNG library application note*» (Cf [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 « SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

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 S3FT9KF/S3FT9KT/S3FT9KS, revision 0 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le 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 scrupuleusement les recommandations et contre-mesures 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[1], 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[2], 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 :

[1] 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.

[2] 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 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_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**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 Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**1**	**3**	3	**4**	**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
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16- bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific ID Dedicated Software, version 1.9, 30th november 2011,* Samsung Electronics Co, Ltd. - *Security Target Lite of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16- bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific ID Dedicated Software, version 1.0, 19th december 2011,* Samsung Electronics Co, Ltd.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report CAHOKIA, reference LETI.CESTI.CAH.RTE.001 du 08/06/2012 – v1.3 – 8thjune 2012,* CEA-LETI. - *Evaluation Technical Report Lite CAHOKIA, reference LETI.CESTI.CAH.RTE_LITE.002-v1.0 – v1.0 – 11thjune 2012,* CEA-LETI.
[CONF]	Liste de configuration du produit - *Project <CAHOKIA>Life Cycle Definition (Class ALC_CMC.4/CMS.5), version 1.5, 2nd December 2011, SAMSUNG .*
[GUIDES]	Guides du produit : - *S3FTKX 16-Bit CMOS MICROCONTROLLERS for Smart Card, reference S3FT9KX_UM_REV1.20, rev 1.20, november 2011*, Samsung Electronics Co, Ltd ; - *Boot Loader Specification for S3FT9Kx Products, version 0.6, 30th september 2011*, Samsung Electronics Co, Ltd ; - *TORNADO-2Mx2 RSA/ECC Library API Manual, reference TN_T2Mx2_RSAECC_APIManual_v3.00, version 3.00, 8th november 2011*, Samsung Electronics Co, Ltd ; - *Application Note DRNG Software Library v1.0 S3FT9Kx family, version 1.0, 11th november 2010,* Samsung Electronics Co, Ltd ; - *S3FT9KX HW DTRNG and DTRNG library application note, revision 1.0, 14th march 2011*, Samsung Electronics Co, Ltd ; - *S3FT9KX HW TRNG and AIS31 online test library application note, revision 1.1, 3rd march 2011*, Samsung Electronics Co, Ltd ; - *Security Application Note for S3FT9KF/KT/KS, version 1.4, 10th november 2011*, Samsung Electronics Co, Ltd ; - *S3FT9KF/KT/KS Chip Delivery Specification, revision 1.1, october 2011*, Samsung Electronics Co, Ltd ; - *Architecture Reference: SecuCalm CPU Core, version AR14, 3rd march 2011*, Samsung Electronics Co, Ltd.
[PP0035]	*Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007*. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* 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 : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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 www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
[AIS 31]	*Functionnality classes and evaluation methodology for physical random number generator*, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).