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-2013/49

Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7, incluant la librairie sécurisée RSA v4.2

Paris, le 19 juillet 2013

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

[Original signé]

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-2013/49

Nom du produit, référence, version

Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7, incluant la librairie sécurisée RSA v4.2

Conformité à un profil de protection

BSI-PP-0035

Security IC Platform Protection Profile, version 1.0 June 2007

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

San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 446-711, République de Corée

Commanditaire

Samsung Electronics Co. Ltd

San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 446-711, 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

Le produit évalué est la famille « Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7, incluant la librairie sécurisée RSA v4.2 » développé par Samsung Electronics Co. Ltd.

Les quatre microcontrôleurs faisant l'objet de ce certificat diffèrent uniquement par la quantité de mémoire Flash disponible.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il peut être inséré dans un support plastique pour constituer une carte à puce. Il est destiné à héberger une ou plusieurs applications S-SIM. Celles-ci 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 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].

La version certifiée du produit est identifiable par lecture de la mémoire « *flash initialization data information* » située à l'adresse 0xC0000-0xC01FF (voir [GUIDES]).

Adresse	Contenu	Valeur attendue
0xC0004 – 0xC0005h	Type	0x0113, 0x0111, 0x11F et 0x0312 pour S3FS91J, S3FS91H, S3FS91V et S3FS93I respectivement.
0xC002A	Révision	0x07
0xC002B	Version du logiciel 'boot loader'	0x10
0xC002C – 0xC002D	Version de la librairie sécurisée RSA	0x042C
0xC002E	Version de la librairie TRNG	0x01

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- détection, enregistrement et réaction aux attaques environnementales ;
- contrôle d'accès ;
- non-réversibilité du changement de mode de « *test* » vers « *user* » (voir §1.2.5) ;
- contre-mesures matérielles pour la non-observabilité ;
- support à la cryptographie.

1.2.4. Architecture

Les produits S3FS91J, S3FS91H, S3FS91V, S3FS93I sont constitués des éléments suivants :

- une partie matérielle composée :
  - d'un processeur RISC 32 bits ARM SC100.
  - de mémoires :
    - de type Flash NOR pour embarquer le code client et contenir les données applicatives :
      - 768Ko pour le S3FS91J ;
      - 650Ko pour le S3FS93I ;
      - 512Ko pour le S3FS91H ;
      - 420Ko pour le S3FS91V.
    - 8Ko de mémoire ROM pour le programme de test et 32Ko de mémoire ROM pour les autres programmes dédiés ;
    - 20Ko de mémoire RAM dont 2Ko de mémoire CRYPTO RAM réservée pour les calculs cryptographiques.
  - de modules de sécurité :
    - module de protection mémoires (MPU) ;
    - module pour le chiffrement / déchiffrement des mémoires ;
    - contrôle d'intégrité à la volée des blocs mémoire et bus (CRC) ;
    - détecteurs de sécurité (température, tension, fréquence, LASER) ;
    - bouclier de protection (*active shield*).
  - de modules fonctionnels :
    - gestion des entrées/sorties suivant les deux interfaces I/O ISO7816 et SWP ;
    - coprocesseur sécurisé DES/TDES ;
    - coprocesseur sécurisé Tornado™ pour le chiffrement asymétrique RSA ;
    - générateurs de nombres aléatoires TRNG.

- des logiciels dédiés (*firmwares*) en ROM intégrant :
  - une bibliothèque pour les calculs arithmétiques modulaires pour le support à la cryptographie asymétrique RSA ;
  - une bibliothèque pour la génération de nombres aléatoires (*TRNG software library*) ;
  - un logiciel de chargement sécurisé (*secure bootloader*) stocké en ROM pour charger du code en mémoire Flash et rediriger définitivement le début du flot d'exécution (*boot*) vers la Flash ;
  - des programmes de tests du microcontrôleur (ces programmes de tests ne font pas partie du périmètre de l'évaluation).

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

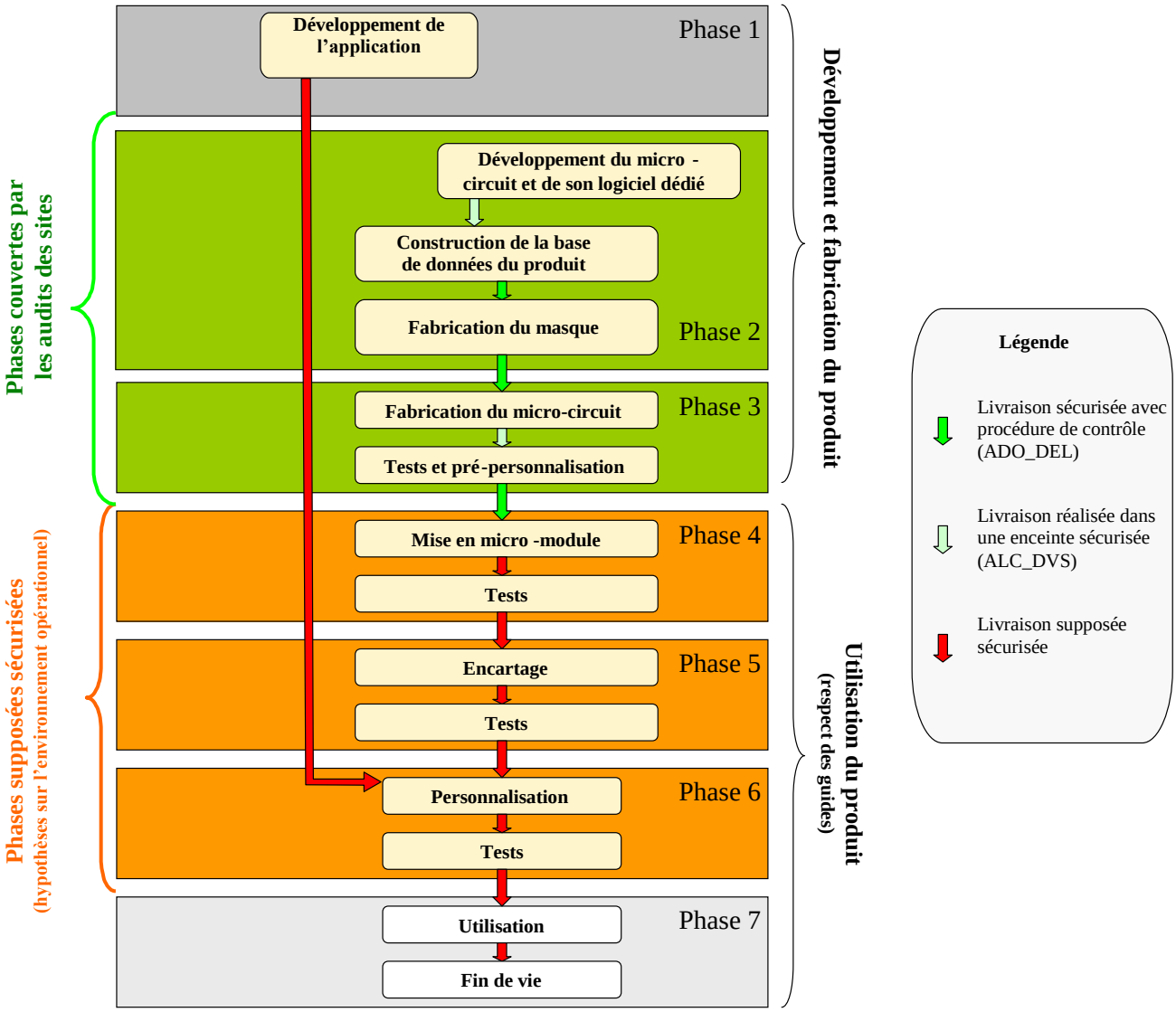

Figure 1 - Cycle de vie du produit

Les produits ont été développés sur les sites suivants :

Giheung Plant

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

Hwasung Plant

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

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

Eternal Plant	**ChangFeng Plant**
No.1755, Hong Mei South Road Shanghai République Populaire de Chine	No. 818, Jin Yu Road Jin Qiao Export Processing Zone, Pudong, Shanghai République Populaire de Chine

Le microcontrôleur comporte deux modes d'utilisation :

- un mode « *test* », dans lequel le fonctionnement du microcontrôleur est testé à l'aide d'un système de test externe. Cette étape est réalisée dans l'enceinte sécurisée du site du développeur. Après la phase de test, le mode « test » est inhibé de façon irréversible. L'interface de test n'est alors plus accessible ;
- un mode « *user* », dans lequel le microcontrôleur fonctionne sous le contrôle des logiciels dédiés et de l'application embarquée de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans ce mode.

En mode « *user* », la puce est soit dans son état initial « *ROM boot* » à partir duquel l'utilisateur peut charger son propre code dans la mémoire « *Flash NOR* », soit dans l'état « *FLASH boot* » dans lequel elle démarre sur le code propre à l'utilisateur déjà chargé en mémoire Flash.

1.2.6. Configuration évaluée

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis en section 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 en section 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3.

Pour les besoins de l'évaluation, le microcontrôleur S3FS91J a été fourni au centre d'évaluation avec un système d'exploitation, logiciel dédié, dans un mode dit « ouvert[1] ». Le CESTI a jugé que le microcontrôleur S3FS91J était représentatif de la famille de produits qui fait l'objet de ce rapport de certification.

[1] Mode permettant de charger et d'exécuter du code natif en Flash et d'activer ou désactiver les mécanismes sécuritaires paramétrables.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

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

L'évaluation s'appuie partiellement sur les résultats d'évaluation liés à la certification de la version précédente du produit [COWICHAN2].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 décembre 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 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 visé.

2.4. Analyse du générateur d'aléas

Le produit évalué offre un générateur de nombres aléatoires constitué d'un générateur physique de nombres aléatoires TRNG, muni d'un retraitement cryptographique non implémenté mais qui est décrit dans le document « *TRNG application note v1.3* » (voir [GUIDES]). Ce générateur TRNG peut être utilisé par le logiciel embarqué.

La conformité du générateur physique de nombres aléatoires TRNG, muni du retraitement cryptographique indiqué dans les guides, au référentiel cryptographique de l'ANSSI (voir [REF]) a été évaluée. Le générateur TRNG atteint le niveau « standard ».
Enfin, durant l'évaluation, le générateur TRNG 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].

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 « Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7, incluant la librairie sécurisée RSA v4.2 » 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 « Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7, incluant la librairie sécurisée RSA v4.2 » 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].

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							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_SPM						**1**	1		
	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_FLR									
	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 S3FS91J/S3FS91H/S3FS91V/S3FS93I 32-bits RISC Microcontroller for Smart Card with SWP, Confidential version 2.2, 4th July 2013, Samsung. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target of S3FS91J/S3FS91H/S3FS91V/S3FS93I 32-bits RISC Microcontroller for Smart Card with SWP, Public version 2.1, 4th July 2013, Samsung.
[COWICHAN2]	Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7, Rapport de certification ANSSI-CC-2009/57, 18 mars 2010, ANSSI.
[RTE]	Rapport technique d'évaluation : - Cowichan2 Evaluation Technical Report, LETI.CESTI.COW2.RTE.001-v5.2, 10 juillet 2013, CEA LETI. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Cowichan2 Evaluation Technical Report_Lite, LETI.CESTI.COW2.RTE_lite.002-v3.2, 10 juillet 2013, CEA LETI.
[CONF]	Configuration Management documentation Cowichan2_ACM_v2.0, 14 December 2012, Samsung.
[GUIDES]	- User's Manual S3FS91J_3I_1H_1V_4J_4I, v4.10, 20 April 2009, Samsung ; - Security Application Note S3FS91J/S93I/S91H/S91V, v1.4, 12 December 2012, Samsung ; - RSA crypto library v4.2 application note, v1.4, 12 December 2012, Samsung ; - RSA library design concept, v1.0, 28 May 2008, Samsung ; - S3FS91J AIS31 TRNG application note, v1.3, 15 September 2012, Samsung ; - Delivery specifications, v3.0, September 2008, Samsung ; - Boot Loader Specification for S3FS91J Family Products, v1.0, 1 October 2010, Samsung.
[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 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.
[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 (RGS_B_1), 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).