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-2009/57

Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7

Paris, le 18 mars 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi 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 de la 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-2009/25

Nom du produit

Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7

Référence/version du produit

Microcontrôleur : S3FS91J/ S3FS91H/ S3FS91V/ S3FS93I - Rév. 7

Librairies logicielles : Test Rom code version 1.0, RSA library version 3.9S, TRNG library version 1.0, Secure Bootloader version 1.0

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 (R3)

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, 449-711, République de Corée

Commanditaire

Samsung Electronics Co. Ltd

San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 449-711, République de Corée

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

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, publié au Journal officiel de la République française. 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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT EVALUE 6
1.2.1. Identification du produit 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 7
1.2.4. Cycle de vie 8
1.2.5. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. TRAVAUX D'EVALUATION 10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 10
2.4. ANALYSE DU GENERATEUR D'ALEAS 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RESTRICTIONS D'USAGE 11
3.3. RECONNAISSANCE DU CERTIFICAT 11
3.3.1. Reconnaissance européenne (SOG-IS) 11
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 13

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 16

1. Le produit

1.1. Présentation du produit

Le produit évalué est le microcontrôleur RISC S3FS91J 32-bit, développé par Samsung Electronics Co. Ltd. L'évaluation prend également en compte les dérivés S3FS91H, S3FS91V et S3FS93I, qui ne diffèrent que par leur taille logique de mémoire Flash (cf. §1.2.3). Le microcontrôleur peut être inséré dans un support plastique pour constituer une carte à puce. Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. 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 évalué

La cible de sécurité définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation. La cible de sécurité [ST] est basée sur le profil de protection [PP0002].

Les microcontrôleurs S3FS91J, S3FS91H, S3FS91V, S3FS93I possèdent deux générateurs de nombres aléatoires : RNG1 et RNG2. Seul le générateur RNG2 est pris en compte au sein du périmètre d'évaluation, comme spécifié dans la cible de sécurité [ST]. Ce générateur est constitué d'un TRNG physique et d'un retraitement cryptographique non implémenté mais dont une mise en œuvre est fournie dans les guides [GUIDES].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [ST].
La version certifiée du produit est identifiable par les éléments suivants :

- microcontrôleur référence : S3FS91J, S3FS91H, S3FS91V, S3FS93I révision 5 ;
- librairies logicielles :
  - « Test ROM Code » version 1.0 ;
  - « RSA Library » version 3.9S ;
  - « TRNG Library » version 1.0 ;
  - « Secure Bootloader » version 1.0.

Le nom du produit, son identifiant et la révision du circuit intégré sont des informations qui peuvent être récupérées par la lecture de la mémoire OTP, aux adresses 00 04 et 00 2A.

1.2.2. 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 des modes « *test* » et « *user* » (cf. §1.2.4) ;
- contre-mesures matérielles pour la non-observabilité ;
- cryptographie.

1.2.3. 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 RNG1 et RNG2 (seul RNG2 est évalué, cf. §2.4) ;

- 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 déterministe de nombres aléatoires (DRNG) ;
  - un logiciel de chargement sécurisé (*secure bootloader*) stocké en ROM pour charger du code en mémoire Flash et rediriger définitivement le chargement (*boot*) vers la Flash (cf. 1.2.4) ;
  - des programmes de tests du microcontrôleur.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

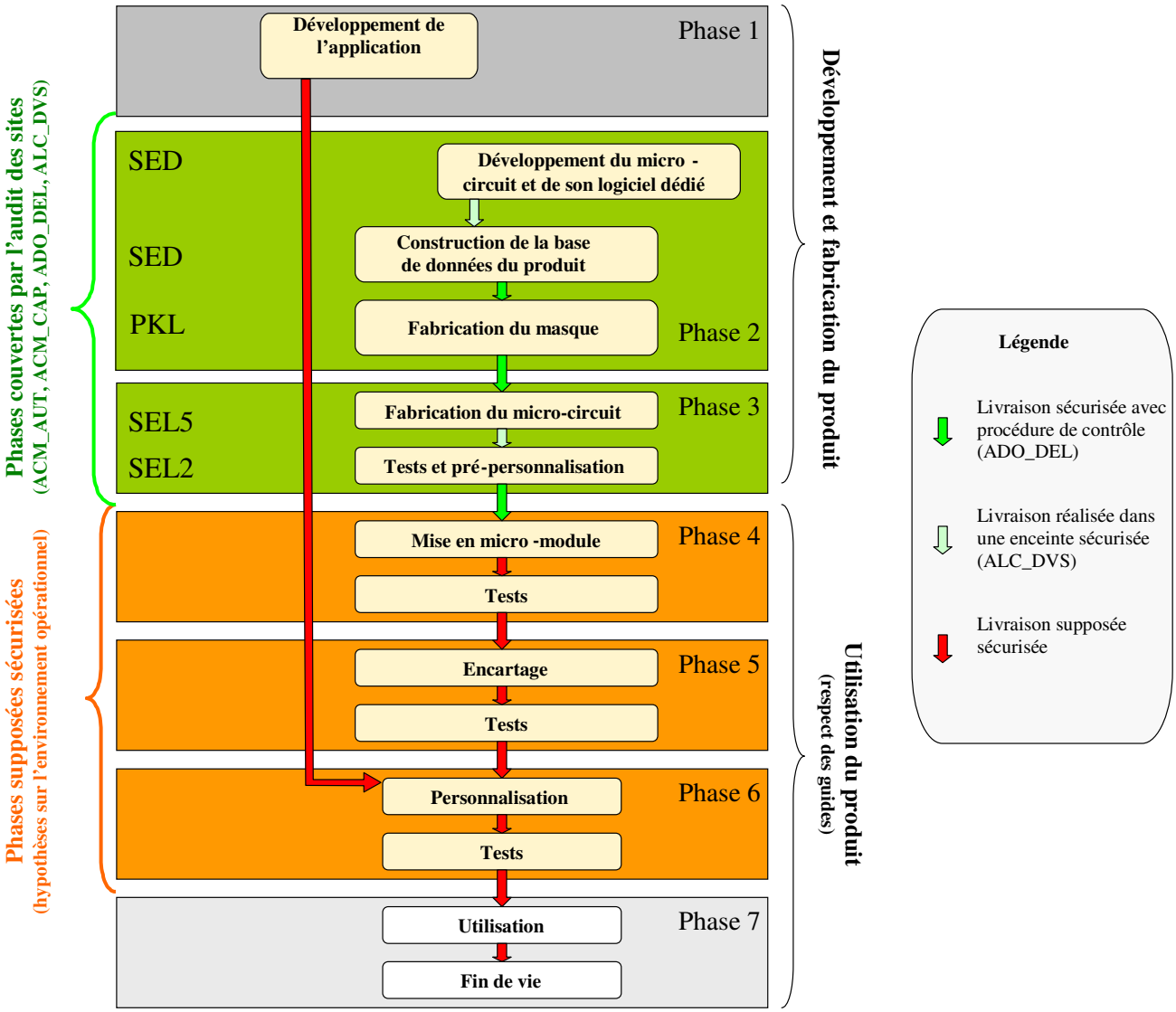

Figure 1 - Cycle de vie du produit

Le design du produit est réalisé par :

Samsung Electronics Co. Ltd - C&M Development team (SED)
San#24 Nongseo-dong, Giheung-gu,
Yongin-City, Gyeonggi-Do, 449-711,
République de Corée

Les réticules du microcontrôleur sont fabriqués par :

PKL (PKL)
493-3 Sungsung-dong, Cheonan-City,
Choongcheongnam-Do, 330-300,
République de Corée

Le produit est fabriqué par :

Samsung Electronics Co. Ltd – Line 5 (SEL5)
San#24 Nongseo-dong, Giheung-gu,
Yongin-City, Gyeonggi-Do, 449-711,
République de Corée

Les échantillons sur galette de silicium (*wafers*) sont testés par :

Samsung Electronics Co. Ltd – Line 2 (SEL2)
San#24 Nongseo-dong, Giheung-gu,
Yongin-City, Gyeonggi-Do, 449-711,
République de Corée

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 Flash.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur seul. Toute application, éventuellement embarquée pour les besoins de l'évaluation, ne fait pas partie du périmètre d'évaluation.

Au regard du cycle de vie, le produit évalué est celui qui sort de la phase de fabrication, tests et pré-personnalisation (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] ».

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

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM]. Pour les composants d'assurance supérieurs au niveau EAL5, des méthodes propres au centre d'évaluation, validées par l'ANSSI et compatibles avec le document [AIS 34], ont été utilisées. Pour répondre aux spécificités des cartes à puce, les guides [CC IC1], [CC IC2] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

La présente réévaluation s'appuie sur les résultats d'évaluation [COW1] issus de la certification CC v2.3 au niveau EAL4+ émise par l'ANSSI en octobre 2009, ainsi que du rapport d'analyse d'impact [IAR] fourni par Samsung.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 1er décembre 2009, 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

Le produit évalué offre des services cryptographiques, identifiés au §1.2.3. Ces services ne peuvent cependant pas être analysés vis-à-vis des référentiels techniques de l'ANSSI [REF-CRY], [REF-CLE] et [REF-AUT] car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépendra de leur emploi par l'application embarquée sur le microcontrôleur qui utilisera éventuellement les fonctions de la librairie *« RSA Library »*, si celle-ci est présente.

2.4. Analyse du générateur d'aléas

Le produit évalué offre un générateur de nombres aléatoires RNG2 (cf. §1.2) 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 v1.1* » (cf. [GUIDES]). Ce générateur RNG2 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 (cf. [REF-CRY]) a été évaluée. Le générateur RNG2 atteint le niveau « standard ».

Le générateur RNG1, conformément à la cible de sécurité [ST], n'intègre pas le périmètre d'évaluation et n'a donc pas été évalué.

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 les produits S3FS91J, S3FS91H, S3FS91V et S3FS93I, en révision 7, soumis à l'évaluation, répond aux caractéristiques de sécurité spécifiées dans la 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 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 spécifiés dans la cible de sécurité [ST] au chapitre 4.2 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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. 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'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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[1], 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 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

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Name of the component
ADV Development	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semiformal 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 Guidance	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedure
ALC Life-cycle support	ALC_CMC		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 Security target evaluation	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claim
	ASE_ECD	1	1	1	1	1	1	1	1	Extended component 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 specifications
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	2	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 Vulnerability assessment	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 : - Cowichan II - Security Target of S3FS91J/S3FS91H/S3FS91V/S3FS93I 32-bits RISC Microcontroller For Smart Card with SWP, Version 1.3, 30 Nov 2009, Samsung Electronics Co. Ltd Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Public - Cowichan II - Security Target of S3FS91J/S3FS91H/S3FS91V/S3FS93I 32-bits RISC Microcontroller For Smart Card with SWP, Version 1.0, 30 Nov 2009, Samsung Electronics Co. Ltd
[RTE]	Rapport technique d'évaluation : - Cowichan – Rapport technique d'évaluation, Référence : LETI.CESTI.Cow2.RTE.001 - v1.0 - 27/11/2009, CESTI LETI Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Cowichan - Evaluation Technical Report – lite, Référence : LETI.CESTI.COW2.RTE.002 - v1.0 – 01/12/2009, CESTI LETI
[COW1]	Rapport de certification issu du projet initial COWICHAN 1 : - Certification CC v2.3 EAL4+ des microcontrôleurs RISC 32-bit SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 5, Référence : ANSSI-CC-2009/25, 15 octobre 2009, ANSSI
[IAR]	Rapport d'analyse d'impact : - Cowichan2 Revision 7 Samsung Action Items, Référence : IAR_cow2_rev7_v1, 16 octobre 2009, Samsung Electronics Co. Ltd

[GUIDES]	Les guides du produit sont constitués des documents suivants : - User's manual, Revision 4.10, Samsung Electronics Co. Ltd - Security Application Note, version 1.2, Samsung Electronics Co. Ltd - TRNG Application Note, Version 1.1, Samsung Electronics Co. Ltd - RSA Application Note, Version 1.1, Samsung Electronics Co. Ltd - RSA Crypto Library Design Concept, Version 1.0 Samsung Electronics Co. Ltd - Delivery specification, Version 1.0, Samsung Electronics Co. Ltd - Test-Administrator's Guidance, Version 1.0, 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 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, CCIMB-2009-07-001 version 3.1R3, 07/2009 ; Part 2: Security functional requirements, CCIMB-2009-07-002 version 3.1R3, 07/2009 ; Part 3: Security assurance requirements, CCIMB-2009-07-003 version 3.1R3, 07/2009.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, CCIMB-2009-07-004 version 3.1R3, 07/2009.
[CC IC1]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 Version 3.0 Revision 1, 03/2009.
[CC IC2]	Common Criteria Supporting Document - Mandatory Technical Document - Requirements to perform Integrated Circuit Evaluations, reference CCDB-2009-03-003 Version 2.0, 03/2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.
[REF-CLE]	Gestion de clés - Règles et recommandations concernant La gestion des clés utilisées dans les mécanismes cryptographiques de niveau de robustesse standard, v1.0 du 28 mars 2006, réf: 724/SGDN/DCSSI/SDS/AsTeC.

[REF-AUT]	Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, v0.13 du 12 avril 2007, réf: 729/SGDN/DCSSI/SDS.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)