PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2021/02

Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (Référence : S3FV9QM_20200504)

Paris, le 15 janvier 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2021/02

Nom du produit

Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software

Référence/version du produit

Référence : S3FV9QM_20200504

Conformité à un profil de protection

Security IC Platform Protection Profile, version 1.0,
certifié BSI-CC-PP-0035-2007 le 23 août 2007

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeur

SAMSUNG ELECTRONICS CO LTD
17 Floor, B-Tower, 1-1, Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud

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 avenue des martyrs,
38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2.

SOG-IS

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, Référence : S3FV9QM_20200504 » développé par SAMSUNG ELECTRONICS CO LTD.

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 conforme au profil de protection [PP0035].

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 » ;
- la bonne exécution de services de sécurité fournis par la « TOE » aux logiciels embarqués ;
- le support à la cryptographie à clés symétriques ;
- le support à la cryptographie à clés asymétriques avec les librairies cryptographiques optionnelles RSA/ECC Library ou RSA/ECC/SHA ;
- Library ;
- le support à la génération de nombres non prédictibles.

1.2.3 *Architecture*

Le produit est constitué de :

- une partie matérielle comprenant :
    - o un processeur 32 bits « *RISC*[1] » ;
    - o des mémoires :

[1] *Reduced Instruction Set Computer* ou processeur à jeu d'instruction réduit.

- 40 Ko de ROM dont 32 Ko pour le stockage des programmes utilisateurs et 8 Ko pour le *Test ROM* ;
- 40 Ko de mémoire RAM dont 35 Ko pour le stockage des données utilisateurs et 5 Ko spécifiques pour le calcul cryptographique ;
- 512 octets de mémoire DMA RAM ;
- FLASH dont 512 octets de mémoire spéciale et :
  - 1280 Ko pour le S3FV9QM ;
  - 1024 Ko pour le S3FV9QK ;

o de modules de sécurité : unité de protection mémoire (*MPU*[2]), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;

o de modules fonctionnels : gestion des entrées/sorties en mode contact (interfaces ISO 7816 et *SWP*[3]), générateur de nombres aléatoires, crypto-processeurs Triple-DES et AES ainsi qu'un accélérateur cryptographique TORNADO-E pour le support d'algorithmes cryptographiques à clés asymétriques,

- une partie logicielle comprenant :

o un logiciel *Test ROM* (hors cible d'évaluation), utilisé par le développeur avant la livraison du produit, inaccessible à l'utilisateur après livraison ;

o un logiciel *Secure Boot Loader*, permettant à l'utilisateur de charger son code en mémoire FLASH ;

o une *Crypto Library* optionnelle et une *DTRNG Librarie* optionnelle, permettant à l'utilisateur de réaliser des calculs RSA, ECC ou SHA et de générer des nombres aléatoires.

1.2.4 *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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.2 « TOE Definition ».

Eléments de configuration			Données d'identification lues
Identification des microcontrôleurs	S3FV9QM		0x1A16
	S3FV9QK		0x1A14
	Revision 3		0x00 ou 0x01
Identification des logiciels embarqués	*Test ROM Code version 1.0*		0x10
	Boot loader code	*version 2.1*	0x21
		version 2.2	0x22
		version 2.6	0x26
Identification des	*DTRNG*	*version 2.0*	0x02

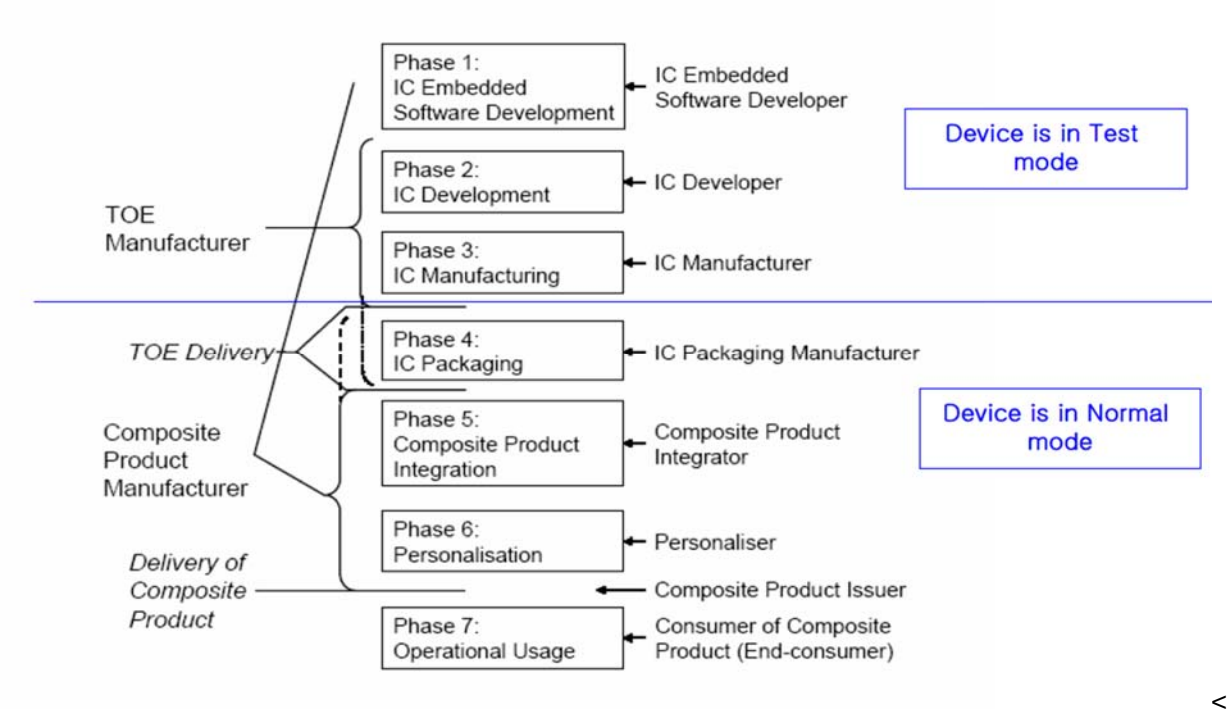
[2] *Memory Protection Unit* ou unité de protection mémoire.

[3] *Single Wire Protocol* ou protocole simple connexion.

bibliothèques	*Library* (optionnelle)	*version 3.0*	0x03
		version 4.0	0x04
	RSA/ECC library version 1.6 (optionnelle)		0x312E36
	RSA/ECC/SHA library version 1.74 (optionnelle)		0x312E3734

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :



<

Le produit a été développé sur les sites suivants (voir [SITES]) :

Nom du Site	Adresse	Fonction
Hwasung Plant/ DSR Building	1, Samsungjeonja-ro, Hwasung-City, Gyeonggi-do, Corée du Sud	Phase 2 : *Smart Card Design Center*
Giheung Plant/SR3 building	San #24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do, Corée du Sud	Phase 3 : *Test program development*
Hwasung Plant/ NRD Building	San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 3 : *Mask Shop*
Giheung Plant/ Line 6, S1	San 24, Nongseo-Dong, Giheung-Gu,	Phase 3 : *Wafer Fabrication*
Giheung Plant/ Line 2		Phase 3 : *Inking / Giheung Wafer Stock*

Giheung Plant/ Line 1	Yongin-City, Gyeonggi-Do 446-711 Corée du Sud	Phase 3 : *Grinding*
Onyang Plant/ Warehouse	San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 4 : *Packing, Warehouse*
Onyang Plant/ Line 2		Phase 3&4 : *Stock, Grinding, Sawing, Packaging, Package Testing*
Onyang Plant/ Line 6		Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
PKL Plant	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : *External Mask Shop*
TOPPAN Plant	91, Wonjeok-ro 290 beongil, Sindun-myeon, Icheonsi, Gyeonggi-do, Corée du Sud	Phase 3 : *External Mask Shop*
HANAMICRON plant	#95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
Inesa Plant	No. 818 Jin Yu Road Jin Qiao Export Processing Zone Pudong, Shanghai, Chine	Phase 3&4 : *Grinding, Sawing, COB*
		Phase 4 : *Packaging, Warehouse*
Eternal Plant	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 3&4 : *Sawing, COB*
		Phase 4 : *Packing, Warehouse*
TESNA Plant	450-2 Mogok-Dong, Pyeungtaek City, Gyeonggi, Corée du Sud	Phase 3 : Wafer *Testing, Pre-personalization*
ASE Korea	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, SIP module assembly*
SFA plant	30,2gongda 7-gil, Seobukgu,Cheonansi,Chungcheongnam-do, Corée du Sud	Phase 3 : *IC Bumping*

1.2.6 *Configuration évaluée*

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au 1.2.3. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.

Au regard du cycle de vie détaillé au chapitre 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3 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 5 [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2 Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du produit « Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Library including specific IC Dedicated Software » certifié le 5 novembre 2018 sous la référence ANSSI-CC-2018/43, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 juillet 2020, 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 a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

2.4 Analyse du générateur d'aléas

Les produits embarquent un DTRNG, incluant un retraitement qui a fait l'objet d'une analyse par le CESTI. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélée de faiblesse.

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation. Le générateur atteint le niveau « PTG.2 ».

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 S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, Référence : S3FV9QM_20200504 » 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 « Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software, Référence : S3FV9QM_20200504 » 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[4], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC

[4] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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 [CCRA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[5] , 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 :

[5] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. 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_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	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 Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**5**	*Advanced methodical vulnerability analysis*

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target of Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software*, version 9.5, 20 juillet 2020, SAMSUNG. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Lite of Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software*, version 9.0, 22 juillet 2020, SAMSUNG.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR)* - CAYUSE-R5, référence : LETI.CESTI.CAYR5.FULL.001, version 1.0, 23 juillet 2020, CEA-LETI. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report (ETR for composition)* - CAYUSE-R5, référence : LETI.CESTI.CAYR5.COMPO.001, version 1.0, 23 juillet 2020, CEA-LETI.
[ANA-CRY]	*CAYUSE-R5 CAYUSE3-R4 Task Report : MECA_CRYPTO.1*, référence : LETI.CESTI.CAYR5 CAY3R4.RT.001, version 1.0, 18 septembre 2020.
[CONF]	Liste de configuration du produit : - CAYUSE 1R5 - Class : ALC_CMC.4/CMS.5 – Life Cycle Definition, référence : Cayuse1R_ALC_CMC_CMS_9.2, version 9.2, 23 juillet 2020, *SAMSUNG.*
[GUIDES]	Guides du produit : - *TORNADO-E RSA/ECC Library API Manual*, version 1.441, 8 juillet 2020, SAMSUNG ; - *TORNADO-E RSA/ECC Library API Manual*, version 1.47, 20 juillet 2020, SAMSUNG ; - *S3FV9xx HW DTRNG and DTRNG library application note*, version 1.6, 8 juillet 2020, SAMSUNG ; - *S3FV9xx HW DTRNG and DTRNG library application note*, version 2.1, 6 juillet 2020, SAMSUNG ; - *S3FV9QM/QK 32-Bit CMOS Microcontroller for Smart Card, User's Manual*, révision 1.11, 5 décembre 2013, SAMSUNG ; - *S3FV9Qx Security Application Note*, version 2.0, 1 juin 2018, SAMSUNG Electronics Co. Ltd ; - *S3FV9QM/QK Chip Delivery Specification*, revision 3.2, mai 2016, SAMSUNG.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la

	réutilisation : - *Site Technical Audit Report (STAR) – Development environment – Hwasung STAR_GihHw_191014_v1.pdf*, 14/10/2019 ; - *Site Technical Audit Report (STAR) – Production Environment - Giheung & Hwasung Factory (FAB 1, FAB 2, FAB 6, FAB S1) STAR_Gih_Hw_190614_v5.pdf*, 14/06/2019 ; - *Site Technical Audit Report (STAR) Onyang STAR_Onyang_180615_v1.pdf*, 15/06/2018 ; - *ALC RE-USE REPORT PKL Cheonan 0882_ALC-Re-Use-Report-ANSSI_PKL_Cheonan_190627_v1.pdf*, 27/06/2019 ; - *Site Technical Audit Report (STAR) HANA Micron Inc. STAR_HANA_Micron_181203_v1.pdf*, 03/12/2018 ; - *ALC RE-USE REPORT INESA Shanghai 1026_ALC-Re-Use-Report-ANSSI_Inesa_Shanghai_180419_v2.pdf*, 19/04/2018 ; - *ALC RE-USE REPORT TESNA Pyeongtaek 1026_ALC-Re-Use-Report-ANSSI_Tesna_Pyeungtaek_180419_v2.pdf*, 19/04/2018 ; - *ASE Korea Site Certificate 2018 BSI-DSZ-CC-S-0106-2018* 15/08/2018 ; - *Site Technical Audit Report (STAR) ASE Korea STAR_ASE_Korea_180615_v1.pdf*, 15/06/2018.
[PP0035]	*Protection Profile, Security IC Platform Protection Profile*, version 1.0, juin 2007. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0035-2007.
[CER]	*« SAMSUNG S3FV9QM / S3FV9QK, révision 3 ».* Certifié par l'ANSSI sous la référence ANSSI-CC-2018/43.

ANNEXE C. 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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 hardware devices with security boxes*, version 3.0, juillet 2020.
[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 www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), 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 (RGS_B3), voir www.ssi.gouv.fr.
[AIS 31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 Septembre 2011, 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.