



**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-2020/71**

**S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC  
Microcontroller for Smart Card with optional AE1  
Secure Libraries including specific IC Dedicated  
software  
(Revision 0 & 1)**

Paris, le 7 octobre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]



## AVERTISSEMENT

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

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

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

Référence du rapport de certification	<b>ANSSI-CC-2020/71</b>
Nom du produit	<b>S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software</b>
Référence/version du produit	<b>Revision 0 &amp; 1</b>
Conformité à un profil de protection	<b><i>Security IC Platform Protection Profile with Augmentation Packages, version 1.0</i></b> certifié BSI-CC-PP-0084-2014 le 19 février 2014 avec conformité aux packages : <i>"Loader dedicated for usage in Secured Environment only"</i> <i>"Loader dedicated for usage by authorized users only"</i>
Critère d'évaluation et version	<b>Critères Communs version 3.1 révision 5</b>
Niveau d'évaluation	<b>EAL 6 augmenté ASE_TSS.2</b>
Développeur	<b>Samsung Electronics Co Ltd.</b> 17 Floor, B-Tower, 1-1, Samsungjeonja-ro Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud
Commanditaire	<b>Samsung Electronics Co Ltd.</b> 17 Floor, B-Tower, 1-1, Samsungjeonja-ro Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud
Centre d'évaluation	<b>CEA - LETI</b> 17 avenue des martyrs, 38054 Grenoble Cedex 9, France
Accords de reconnaissance applicables	  <p>Ce certificat est reconnu au niveau EAL2.</p>

## 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](http://www.ssi.gouv.fr).

## TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit .....	6
1.2.1	Introduction .....	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture .....	6
1.2.4	Identification du produit .....	7
1.2.5	Cycle de vie .....	8
1.2.6	Configuration évaluée .....	9
2	L'évaluation.....	10
2.1	Référentiels d'évaluation .....	10
2.2	Travaux d'évaluation .....	10
2.3	Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	10
2.4	Analyse du générateur d'aléas.....	10
3	La certification .....	12
3.1	Conclusion.....	12
3.2	Restrictions d'usage.....	12
3.3	Reconnaissance du certificat.....	13
3.3.1	Reconnaissance européenne (SOG-IS).....	13
3.3.2	Reconnaissance internationale critères communs (CCRA).....	13
ANNEXE A.	Niveau d'évaluation du produit.....	14
ANNEXE B.	Références documentaires du produits évalué.....	15
ANNEXE C.	Références liées à la certification.....	17

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software, Revision 0 & 1 » 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 strictement conforme au profil de protection [PP0084], avec :

- le *package* « loader dedicated for usage in secured environment only » ;
- le *package* « loader dedicated for usage by authorized users only ».

### 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 et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ou asymétriques ;
- le support à la génération de nombres non prédictibles.

### 1.2.3 Architecture

Le produit est constitué des éléments suivants :

- une partie matérielle comprenant :
  - o un processeur 32 bits « RISC<sup>1</sup> » ;
  - o des mémoires :
    - 48 Ko de ROM ;
    - 55 Ko de RAM dont 5 Ko dédiés au coprocesseur arithmétique et 2 Ko de cache ;

---

<sup>1</sup> *Reduced Instruction Set Computer* ou processeur à jeu d'instructions réduit.

- 2000, 1768, 1536 et 1024 Ko de FLASH respectivement pour les modèles S3FV9RR, S3FV9RQ, S3FV9RP et S3FV9RK ;
  - des modules de sécurité : protection de la mémoire (MPU), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
  - des modules fonctionnels : gestion des entrées / sorties en mode contact (UART, SWP et SPI), génération de nombres aléatoires – DTRNG (*Digital True Random Number Generator*<sup>2</sup>) et BPRNG (*Bilateral Pseudo-Random Number Generator*) à usage interne uniquement, coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO-E ;
- une partie logicielle composée :
  - des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
  - de bibliothèques pour la génération de nombres aléatoires *DTRNG FRO M library*, version 2.0 et version 2.1 ;
  - de bibliothèques pour la cryptographie asymétrique *AE1 Secure RSA library*, version 2.02 ;
  - de la bibliothèque *AE1 Secure RSA/ECC/SHA Library*, version 2.03 ;
  - d'un *Secure Boot Loader et system API*, version 1.4, permettant le chargement sécurisé du code utilisateur.

#### 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 1.2.2« TOE Definition ».

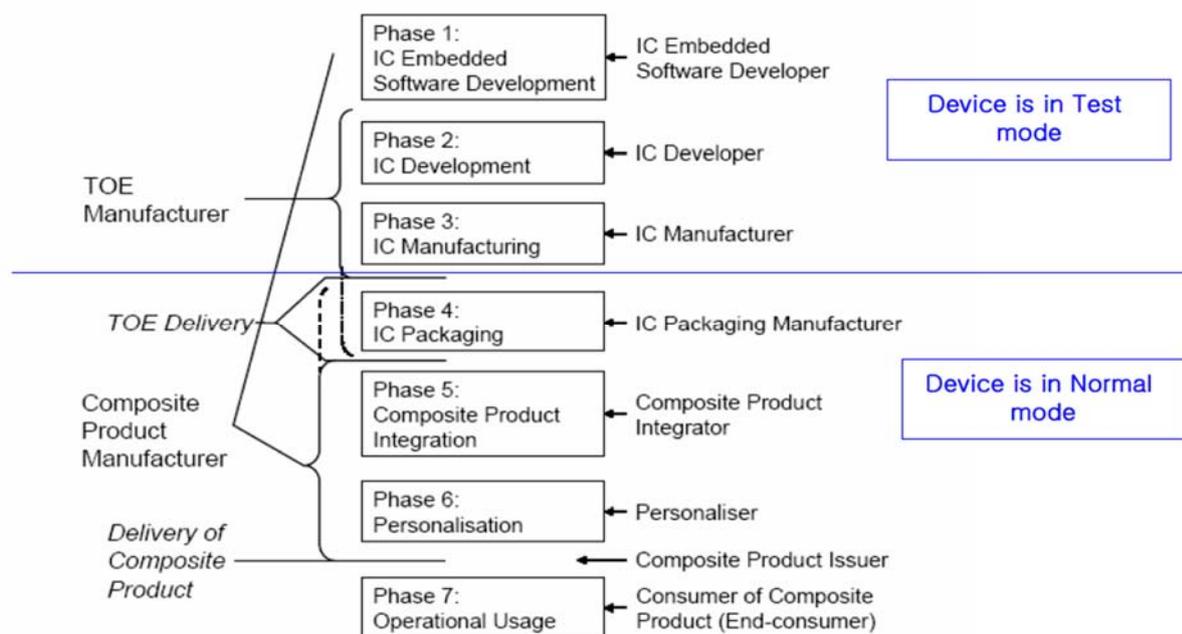
Eléments de configuration		Données d'identification lues
Identification du microcontrôleur	S3FV9RR	0x1B1B
	S3FV9RQ	0x1B1A
	S3FV9RP	0x1B19
	S3FV9RK	0x1B14
	Revision 0 ou 1	0x00 ou 0x01
Identification des logiciels embarqués	Test ROM Code version 1.0	0x10
	Secure Boot loader and system API version 1.4	0x14
Identification des bibliothèques	DTRNG FRO M library version 2.0	0x0200
	DTRNG FRO M library version 2.1	0x0201
	AE1 Secure RSA library version 2.02	En ASCII 'PKA_Lib_AE1_v2.02'
	AE1 Secure RSA library version 2.03	En ASCII 'PKA_Lib_AE1_v2.03'

<sup>2</sup> Générateur physique de nombres aléatoires.

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide S3FV9RR - Chip Delivery Specification (voir [GUIDES]).

### 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 : <i>Smart Card Design Center</i> Phase 3 : <i>Test program development</i>
Hwasung Plant/ NRD/MR2 Building	San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 3 : <i>Mask Shop</i>
Giheung Plant/ Line S1	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 446-711 Corée du Sud	Phase 3 : <i>Wafer Fabrication</i>
Giheung Plant/ Line 2		Phase 3 : <i>Inking / Giheung Wafer Stock</i>
Giheung Plant/ Line 1		Phase 3 : <i>Grinding</i>
Onyang Plant/ Warehouse	San #74, Buksoo-Ri, Baebang-	Phase 4 : <i>Packing, Warehouse</i>

Onyang Plant/ Line 2	Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : <i>Stock, Grinding, Sawing, Packaging, Package Testing</i>
Onyang Plant/ Line 4		Phase 3&4 : <i>Grinding, Sawing, Packaging, Package Testing</i>
PKL Plant	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : <i>External Mask Shop</i>
HANAMICRON plant	#95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : <i>Grinding, Sawing, Packaging, Package Testing</i>
Inesa Plant	No. 818 Jin Yu Road Jin Qiao Export Processing Zone Pudong, Shanghai, Chine	Phase 3&4 : <i>Grinding, Sawing, COB</i>
		Phase 4 : <i>Packaging, Warehouse</i>
Eternal Plant	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 3&4 : <i>Sawing, COB</i>
		Phase 4 : <i>Packing, Warehouse</i>
TESNA Plant	450-2 Mogok-Dong, Pyeongtaek City, Gyeonggi, Corée du Sud	Phase 3 : <i>Wafer Testing, Pre-personalization</i>
ASE Korea	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : <i>Grinding, Sawing, SIP module assembly</i>
SFA Plant	30,2 gongda 7-gil, Seobukgu, Cheonansi, Choongcheongnam-Do, Corée du sud	Phase 4 : <i>IC Bumping</i>

### 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 « S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software » certifié le 19 octobre 2018 sous la référence ANSSI-CC-2018/40, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 07/07/2020, 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, appelé DTRNG FRO M, 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 révélé 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 « S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software, Revision 0 & 1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 6 augmenté du composant ASE\_TSS.2.

#### 3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit « S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software, Revision 0 & 1 » 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 ce micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

### 3.3 Reconnaissance du certificat

#### 3.3.1 Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord<sup>3</sup>, 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 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<sup>4</sup>, des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC\_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



<sup>3</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.eu](http://www.sogis.eu).

<sup>4</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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 6+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	3	Minimally complex structured internals
	ADV_SPM						1	1	1	1	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	5	5	Complete semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	5	5	Advanced support
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	3	3	Compliance with implementation standards – all parts
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	2	2	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		1	2	2	2	3	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	2	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	2	Ordered functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

## ANNEXE B. Références documentaires du produits évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software, ST (Security Target), version 5.2, 07/07/2020, SAMSUNG.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Libraries including specific IC Dedicated software, ST (Security Target) Lite, version 5.0, 07/07/2020, SAMSUNG.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report (full ETR) – CAYUSE3R4 – LETI.CESTI.CAY3R4.FULL.001, version 1.0, 07/07/2020, CEA-LETI.</li> </ul> <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"> <li>- -Evaluation Technical Report for Composition – CAYUSE3R4, LETI.CESTI.CAY3R4.COMPO.001, version 1.0, 07/07/2020, CEA-LETI.</li> </ul>
[ANA-CRY]	<p>CAYUSE-R5 CAYUSE3-R4 Task Report : MECA_CRYPT0.1, référence : LETI.CESTI.CAYR5 CAY3R4.RT.001, version 1.0, 18/09/2020.</p>
[CONF]	<p>Liste de configuration du produit :</p> <p>Common Criteria Information Technology Security Evaluation – Cayuse3R4 – Configuration Management, référence : Cayuse3R4_ALC_CMC_CMS_V5, version 5, 07/07/2020, SAMSUNG.</p>
[GUIDES]	<p>Guides du produit :</p> <ul style="list-style-type: none"> <li>- S3FV9RX HW DTRNG FRO M and DTRNG FRO M Library Application Note, version 1.12, 02/07/2020, SAMSUNG ;</li> <li>- S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note, version 1.2, 01/11/2019 ;</li> <li>- AE1 RSA Library API Manual for AE1 Secure RSA/SHA, version 0.11, 29/06/2020, SAMSUNG ;</li> <li>- RSA/ECC Library API Manual (AE1 RSA ECC Library API Manual v1.02), version 1.02, 01/07/2020, SAMSUNG ;</li> <li>- User's Manual - S3FV9Rx – 32-Bit CMOS Microcontroller for Smart Card, version 2.01, 10/04/2017, SAMSUNG ;</li> <li>- Security Application Note for S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK, S3NSN4V, Version 0.9, 25/10/2019</li> <li>- S3FV9RR - Chip Delivery Specification, version 1.0, février 2016, SAMSUNG ;</li> <li>- Technical Notification - Boot loader Specification for S3FV9Rx, version 1.15, 23/03/2016, SAMSUNG ;</li> <li>- Application Note - S3FV9Rx – System API, version 1.2, 12/02/2016, SAMSUNG ;</li> <li>- SC300 Reference Manual, version 0.0, 12 mai 2014, SAMSUNG.</li> </ul>
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> <li>- Site Technical Audit Report (STAR) – Development environment – Hwasung STAR_GihHw_191014_v1.pdf, 14/10/2019 ;</li> </ul>

	<ul style="list-style-type: none"> <li>- Site Technical Audit Report (STAR) – Production Environment - Giheung &amp; Hwasung Factory (FAB 1, FAB 2, FAB 6, FAB S1) STAR_Gih_Hw_190614_v5.pdf, 14/06/2019 ;</li> <li>- Site Technical Audit Report (STAR) Onyang STAR_Onyang_180615_v1.pdf, 15/06/2018 ;</li> <li>- ALC RE-USE REPORT PKL Cheonan 0882_ALC-Re-Use-Report-ANSSI_PKL_Cheonan_190627_v1.pdf 27/06/2019 ;</li> <li>- Site Technical Audit Report (STAR) HANA Micron Inc. STAR_HANA_Micron_181203_v1.pdf 03/12/2018 ;</li> <li>- ALC RE-USE REPORT INESA Shanghai 1026_ALC-Re-Use-Report-ANSSI_Inesa_Shanghai_180419_v2.pdf 19/04/2018 ;</li> <li>- ALC RE-USE REPORT TESNA Pyeongtaek 1026_ALC-Re-Use-Report-ANSSI_Tesna_Pyeongtaek_180419_v2.pdf 19/04/2018 ;</li> <li>- ASE Korea Site Certificate 2018 BSI-DSZ-CC-S-0106-2018 15/08/2018</li> <li>- Site Technical Audit Report (STAR) ASE Korea STAR_ASE_Korea_180615_v1.pdf 15/06/2018.</li> </ul>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</p>

## 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]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none"> <li>- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;</li> <li>- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;</li> <li>- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document - The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[JIWG AP] *	<i>Mandatory Technical Document - Application of attack potential to smartcards</i> , version 3.0, avril 2019.
[CC RA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
	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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
	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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[AIS 31]	<i>A proposal for: Functionality classes for random number generators, AIS20/AIS31</i> , version 2.0, 18 Septembre 2011, BSI ( <i>Bundesamt für Sicherheit in der Informationstechnik</i> ).

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