



**PREMIÈRE  
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-2023/32

**S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK  
(S3FV9RR\_20230407)**

Paris, le 04 Juillet 2023

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

Vincent STRUBEL

[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-2023/32</b>
Nom du produit	<b>S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK</b>
Référence/version du produit	<b>S3FV9RR_20230407</b>
Conformité à un profil de protection	<b>Security IC Platform Protection Profile with Augmentation Packages, version 1.0</b> certifié BSI-CC-PP-0084-2014 le 19 février 2014 avec conformité aux packages : "Authentication of the security IC" "Loader dedicated for usage in Secured Environment only" "Loader dedicated for usage by authorized users only" "TDES", "AES", "Hash functions"
Critère d'évaluation et version	<b>Critères Communs version 3.1 révision 5</b>
Niveau d'évaluation	<b>EAL6 augmenté</b> ASE_TSS.2
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 1-1 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	  Ce certificat est reconnu au niveau EAL2.

## 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.....	6
1.2.5	Cycle de vie .....	6
1.2.6	Configuration évaluée .....	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation .....	8
2.2	Travaux d'évaluation .....	8
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	8
2.4	Analyse du générateur d'aléa.....	8
3	La certification .....	9
3.1	Conclusion.....	9
3.2	Restrictions d'usage .....	9
3.3	Reconnaissance du certificat.....	10
3.3.1	Reconnaissance européenne (SOG-IS).....	10
3.3.2	Reconnaissance internationale critères communs (CCRA).....	10
ANNEXE A.	Références documentaires du produit évalué .....	11
ANNEXE B.	Références liées à la certification .....	13

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est la famille de microcontrôleurs « S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK, S3FV9RR\_20230407 » développés par SAMSUNG ELECTRONICS CO. LTD. La seule différence entre eux est la taille logique de mémoire *flash*.

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 « *authentication of the security IC* » ;
- le package « *loader dedicated for usage in secured environment only* » ;
- le package « *loader dedicated for usage by authorized users only* » ;
- les packages de services cryptographiques "TDES", "AES", "Hash functions".

### 1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont mentionnés au chapitre 1.2.2, paragraphe 14 de la cible de sécurité [ST].

### 1.2.3 Architecture

Les éléments matériels et logiciels constitutifs du produit sont décrits au chapitre 1.2.2 de la cible de sécurité [ST].

### 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 valeurs de version indiquées en table 1 de la cible de sécurité, pour chacun de ses composants.

Les versions des composants hardware et software peuvent être vérifiés par lecture des registres spécifiés dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide « *S3FV9RR Chip Delivery Specification* ».

### 1.2.5 Cycle de vie

Le cycle de vie du produit est décrit au chapitre 1.2.4 de [ST], il est conforme au cycle de vie en sept phases décrit dans le profil de protection [PP0084].

### 1.2.6 Configuration évaluée

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au chapitre 1.2 de la cible [ST]. 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, 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 (micromodules, etc.)

## 2 L'évaluation

### 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 12 juin 2023, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

### 2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

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 d'assurance visé.

### 2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant visé. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées dans les guides [GUIDES] doivent être suivies.

Dans le cas où le générateur d'aléa serait utilisé à des fins cryptographiques, il est obligatoire de le combiner à un mécanisme algorithmique de génération de pseudo-aléa, de nature cryptographique, afin de fournir des données aléatoires cryptographiquement satisfaisantes, comme énoncé dans le document [ANSSI Crypto].

Ce générateur d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31] et suivant les dispositions décrites dans la note d'application [CC-NOTE-24].



### **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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

#### **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 microcontrôleur 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>1</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>2</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>1</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>2</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. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- <i>Security Target of Samsung S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK</i>, référence ST_Cayuse3-R8_v9.7, version 9.7, 14 avril 2023.</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>- <i>ST (Security Target) Lite of Samsung S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK</i>, référence ST_Lite_S3FV9RR_RQ_RP_RK_v9.3, version 9.3, 18 avril 2023.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- <i>Evaluation Technical Report (full ETR) – CAYUSE3-R8</i>, référence LETI.CESTI.CAY3R8.FULL.001 – V1.1, version 1.1, 12 juin 2023.</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>- <i>Evaluation Technical Report (ETR for composition) – CAYUSE3-R8</i>, référence LETI.CESTI.CAY3R8.COMPO.001 – V1.1, version 1.1, 12 juin 2023.</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <p><i>Cayuse3R8 – Configuration Management (Class ALC_CMC.5/CMS.5)</i>, référence Cayuse3R8_ALC_CMC_CMS_V9.1, version 9.1, 18 avril 2023.</p>
[GUIDES]	<p>Guide du produit :</p> <ul style="list-style-type: none"> <li>- <i>DTRNG FRO M Application Note</i>, référence S3FV9RR_DTRNG_FRO_M_AN_v1.13, version 1.13, 9 mars 2021 ;</li> <li>- <i>S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note</i>, référence S3FV9RR_S3NSN4V_DTRNG_FRO_M_AN_v1.3, version 1.3, 9 mars 2021 ;</li> <li>- <i>S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note</i>, référence S3FV9RR_S3NSN4V_DTRNG_FRO_M_AN_v2.1, version 2.1, 9 mars 2021 ;</li> <li>- <i>S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note</i>, référence S3FV9RR_S3NSN4V_DTRNG_FRO_M_AN_v3.0, version 3.0, 9 mars 2021 ;</li> <li>- <i>AE1 RSA Library API Manual for AE1 Secure RSA/SHA</i>, référence AES1 RSA ECC Library API Manual v0.111, version 0.111, 20 janvier 2023 ;</li> <li>- <i>TORNADO-E RSA/ECC Library API Manual</i>, référence AES1 RSA ECC Library API Manual v1.021, version 1.021, 20 janvier 2023 ;</li> <li>- <i>TORNADO-E RSA/ECC Library API Manual</i>, référence AES1 RSA ECC Library API Manual v1.041, version 1.041, 20 janvier 2023 ;</li> </ul>

	<ul style="list-style-type: none"><li>- <i>TORNADO-E RSA/ECC Library API Manual</i>, référence AES1 RSA ECC Library API Manual v3.011, version 3.011, 20 février 2023 ;</li><li>- <i>S3FV9Rx User's Manual</i>, référence S3FV9Rx_UM_REV2.01, version 2.01, 10 avril 2017 ;</li><li>- <i>Security Application Note for S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK, S3NSN4V</i>, référence SAN_S3FV9RR_S3NSN4V_v1.5, version 1.5, 16 février 2023 ;</li><li>- <i>S3FV9RR Chip Delivery Specification</i>, référence DeliverySpec_S3FV9RR_Re_v1.0, version 1.0, février 2016 ;</li><li>- <i>Bootloader user's manual for S3FV9RR</i>, référence S3FV9RR_TN02_Bootloader_Specification_v1.15, version 1.15, 23 mars 2016 ;</li><li>- <i>S3FV9RR system API Application Note</i>, référence S3FV9RR_AN01_SystemAPI_v1.2, version 1.2, 12 février 2016 ;</li><li>- <i>SC300 Reference Manual</i>, référence SC300_Reference_Manual_v0.0, version 0.0, 12 mai 2014 ;</li><li>- <i>Cryptographic Mechanisms for S3FV9RR</i>, référence Cryptographic_Mechanisms_S3FV9RR_v0.1, version 0.1, 20 février 2023.</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 B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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 and similar devices</i> , version 3.2, novembre 2022.
[CCRA]	<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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[AIS20/31]	<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.