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-2021/62

## Secure Element S3B512C/SC3512C (32-bit RISC Microcontroller) with optional AT1 Secure Library and Fingerprint Library including specific IC Dedicated software (Référence S3B512C_20210830)

Paris, le 27 décembre 2021

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 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-2021/62**

Nom du produit

**Secure Element S3B512C/SC3512C (32-bit RISC Microcontroller) with optional AT1 Secure Library and Fingerprint Library including specific IC Dedicated software**

Référence/version du produit

**S3B512C_20210830**

Conformité à un profil de protection

***Security IC Platform Protection Profile with Augmentation Packages, version 1.0***

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"*

Critère d'évaluation et version

**Critères Communs version 3.1 révision 5**

Niveau d'évaluation

**EAL 6 augmenté**
**ASE_TSS.2**

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**

**SOG-IS**


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.

# 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 ..... 7
1.2.4 Identification du produit ..... 7
1.2.5 Cycle de vie ..... 8
1.2.6 Configuration évaluée ..... 8
2 L'évaluation ..... 9
2.1 Référentiels d'évaluation ..... 9
2.2 Travaux d'évaluation ..... 9
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI ..... 9
2.4 Analyse du générateur d'aléa ..... 9
3 La certification ..... 10
3.1 Conclusion ..... 10
3.2 Restrictions d'usage ..... 10
3.3 Reconnaissance du certificat ..... 11
3.3.1 Reconnaissance européenne (SOG-IS) ..... 11
3.3.2 Reconnaissance internationale critères communs (CCRA) ..... 11
ANNEXE A. Références documentaires du produit évalué ..... 12
ANNEXE B. Références liées à la certification ..... 13

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est le « *Secure Element S3B512C/SC3512C (32-bit RISC Microcontroller) with optional AT1 Secure Library and Fingerprint Library including specific IC Dedicated software, référence S3B512C_20210830* » 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 du *Secure Element* (SE). Les usages possibles sont multiples (applications bancaires, applications pour le commerce électronique, documents d'identité sécurisés, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

De plus, le microcontrôleur inclut trois IP : le *Secure Processor* (SP), le capteur *Fingerprint* et le *Secure Element* (SE). Ces trois IP sont physiquement séparés et seul le SE IP fait partie du périmètre d'évaluation (TOE[1]).

## 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* ».

### 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 ;
- le *mailbox* permettant la communication entre les deux IP SE et SP.

[1] *Target Of Evaluation.*

*Architecture*

Le produit est décrit au chapitre 1.2 « *TOE Overview and TOE Description* ».
La figure 1 synthétise un aperçu du composant S3B512C/SC3512C.

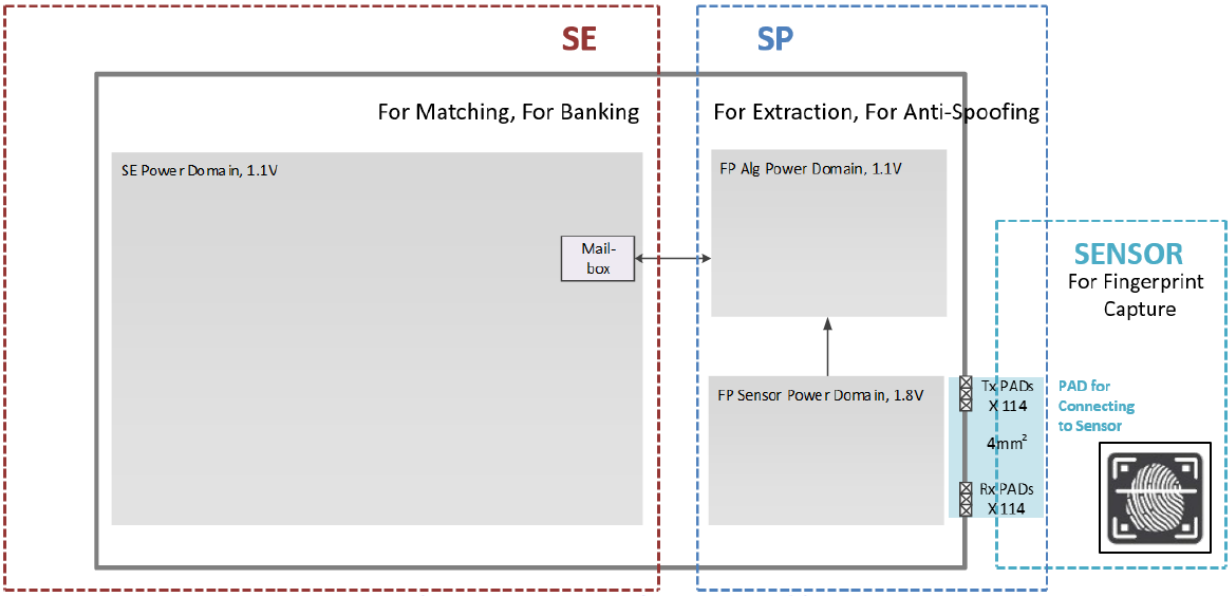


**Figure 1 - Architecture S3B512C/SC3512C**

### 1.2.3 *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* ». Il est à noter que la TOE des composants S3B512C et SC3512C est la même.

| Eléments de configuration | | Données d'identification lues |
|---|---|---|
| Révision matérielle, version 1 | | 0x01 |
| Identification du microcontrôleur | S3B512C | 0x0B0501020CH |
| Identification des logiciels embarqués | *Test ROM Code version 1 (out of the TOE)* | 0x10 |
| | *Secure Boot Loader version 0.1* | 0x01 |
| Identification des bibliothèques | *APT1 RSA/ECC/SHA Library version 1.00 (optional)* | *PKA_Lib_ATP1_v1.00* |
| | *DTRNG FRO M Library version 1.3 (optional)* | *0x0103* |
| | *Fingerprint library v0.4 (optional & out of the TOE)* | *0x04* |

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 « *Chip Delivery Specification* » (voir [GUIDES]-[CDS]).

### 1.2.4 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 1.2.4 de [ST], il est conforme à celui décrit dans le [PP0084]. Le produit a été développé sur les sites décrits dans ce même chapitre, qui sont des sites certifiés par des CESTI du SOG-IS.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le développeur de l'application à embarquer dans le microcontrôleur.

### 1.2.5 *Configuration évaluée*

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au chapitre 1.2.4. 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 mentionné au chapitre 1.2.4 de [ST], 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.

# 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 jour de sa finalisation par le CESTI (voir date en bibliographie), 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]-[Reco_Crypto] afin d'utiliser le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

## 2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa, appelé DTRNG FRO M, qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01]. Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

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 [ANSSI Crypto], 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'aléa n'a pas révélé de faiblesse.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

Ce générateur d'aléa DTRNG FRO M a aussi été analysé conformément à la méthode d'évaluation [AIS31] et suivant les dispositions décrites dans la note d'application [NOTE-24]. Lorsqu'il est utilisé comme indiqué dans [GUIDES]-[DTRNG], il répond aux exigences PTG.2 de la méthodologie [AIS31].

# 3 La certification

## 3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit 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[2], 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[3] , 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 :

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

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

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation : *Security Target of Secure Element S3B512C/SC3512C (32-bit RISC Microcontroller) with optional AT1 Secure Library and Fingerprint Library including specific IC Dedicated software*, référence ST_CREEK_v0.7, version 0.7, 27 août 2021.<br><br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : *ST (Security Target) Lite of Secure Element S3B512C/SC3512C (32-bit RISC Microcontroller) with optional AT1 Secure Library and Fingerprint Library including specific IC Dedicated software*, référence ST_lite_S3B512C_v0.1, version 0.1, 27 août 2021. |
| [RTE] | Rapport technique d'évaluation : *Evaluation Technical Report (full ETR) - CREEK*, référence LETI.CESTI.CRE.FULL.001 - V1.0, 1er septembre 2021.<br><br>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)* - CREEK, référence LETI.CESTI.CREEK.COMPO.001-v1.0, 1er septembre 2021. |
| [CONF] | Liste de configuration du produit : *CREEK Configuration Management (class ALC_CMC.5/CMS.5), référence CRE_ALC_CMC_CMS_V1.0,* 27 août 2021. |
| [GUIDES] | [DTRNG] *S3B512C HW DTRNG FRO M and DTRNG FRO M Library v1.3 Application Note*, référence S3B512C_DTRNG_FRO_M_AN_v1.3, 10 août 2021 ;<br><br>*RSA/ECC/SHA Library API Manual (ATP1 RSA ECC SHA Library API Manual v1.03*), référence ATP1 RSA ECC Library API Manual v1.03, 20 août 2021 ;<br><br>*S3B512C Fingerprint Library Coding Guidance*, référence TN003_B512C_Fingerprint_Library_Coding_Guidance, août 2021 ;<br><br>*User's manual S3B512C SE Secure Element CMOS Microcontroller for Smart Card (Supported Devices: S3B512C*),<br>référence S3B512C_UM_REV0.03, juin 2021 ;<br><br>*Security Application Note For S3B512C Secure Element*, référence SAN_S3B512C_v0.4, 10 août 2021 ;<br><br>[CDS] *S3B512C/SC3512C Chip Delivery Specification*, référence S3B512C SC3512C Family_DV02, juillet 2021 ;<br><br>*S3B512C Bootloader Specification*, référence S3B512C_Bootloader_Specification_ v0.2, 21 juin 2021<br><br>*SC000 Reference Manual*, référence SC000_Reference_Manual v0.0, 13 octobre 2016 ;<br><br>[Reco_Crypto] *Cryptographic Mechanisms For S3B512C,*<br>référence Cryptographic_Mechanisms_S3B512C_v0.0, 12 juillet 2021. |
| [PP0084] | *Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0084-2014. |

# 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 4.0. |
| [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] | *Common Criteria for Information Technology Security Evaluation:*<br>- *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;<br>- *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;<br>- *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 smartcards and similar devices*, version 3.1, juin 2020. |
| [CCRA] | *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. |
| [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. |
| [AIS31] | *A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*). |
| [NOTE-24] | *Note d'application : Evaluations de générateurs d'aléa selon AIS20/AIS31 dans le schéma français, référence ANSSI-CC-NOTE-24_1.0, 2 mars 2021.* |

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