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-2024/26-R01

S3SSE2A (S3SSE2A_20250522)

Paris, le 1/10/2025 | 09:40 CEST

Vincent Strubel

SÉCURITÉ CERTIFICATION

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

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 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.cyber.gouv.fr.

TABLE DES MATIERES

1 Résumé

Référence du rapport de certification **ANSSI-CC-2024/26-R01**
Nom du produit **S3SSE2A**
Référence/version du produit **S3SSE2A_20250522**
Type de produit **Cartes à puce et dispositifs similaires**
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", "TDES", "AES", "Hash functions"* *"Loader dedicated for usage in Secured Environment only"* *"Loader dedicated for usage by authorized users only"*
Critère d'évaluation et version **Critères Communs version CC:2022, révision 1**
Niveau d'évaluation Cible d'évaluation globale : **EAL5 augmenté** ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 Sous-parties de la cible d'évaluation : *Memory Access Control, Bootloader access control, Security detector's reaction to security incidents, Non-reversibility of TEST mode:* **EAL6 augmenté** ASE_TSS.2
Référence du rapport d'évaluation *Evaluation Technical Report (full ETR) – LUMBEE3-R1,* Référence LETI.CESTI.LUM3R1.FULL.001 Version 1.2, 27 août 2025
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Exigences de configuration du produit voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage

Développeur

SAMSUNG ELECTRONICS CO. LTD

Security Product Development Team, 17th floor, B-Tower, DSR Building,
Samsungjeonja-ro 1-1, Hwaseong-si, Gyeonggi-do,
South Korea 445-330

Commanditaire

SAMSUNG ELECTRONICS CO. LTD

Security Product Development Team, 17th floor, B-Tower, DSR Building,
Samsungjeonja-ro 1-1, Hwaseong-si, Gyeonggi-do,
South Korea 445-330

Centre d'évaluation

CEA - LETI

17 avenue des martyrs,
38054 Grenoble Cedex 9, France

CCRA

Ce certificat est reconnu au niveau EAL2.

SOG-IS

2 Le produit

2.1 Présentation du produit

Le produit évalué est « S3SSE2A, S3SSE2A_20250522 » 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.

2.2 Description du produit

2.2.1 *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* « *TDES* » ;
- le *package* « *AES* » ;
- le *package* « *Hash functions* » ;
- le *package* « *loader dedicated for usage in secured environment only* » ;
- le *package* « *loader dedicated for usage by authorized users only* ».

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits au chapitre « *1.2.2 TOE Definition* » de la cible de sécurité [ST].

2.2.3 *Architecture*

Ce produit peut être décomposé en deux parties distinctes : une partie logicielle et une partie matérielle.

Le produit est constitué des composants présentés au chapitre 1.2 « *TOE Overview and TOE Description* » de la cible de sécurité [ST].

2.2.4 *Identification du produit*

Le produit est identifiable par lecture de registres comme indiqué dans les [GUIDES]. La version certifiée correspond aux valeurs indiquées dans la « *Table 1 TOE Configuration »* au chapitre « *1.2.2 TOE Definitions* » de la cible de sécurité [ST].

2.2.5 *Cycle de vie*

Le cycle de vie du produit est le cycle de vie décrit dans [PP0084]. Il est décrit au chapitre 1.2.3 « *TOE Life cycle* » de la cible de sécurité [ST] et la liste des sites impliqués est présentée dans la table 3 « *Sites of the TOE life cycle* ».

2.2.6 *Configuration évaluée*

Le certificat porte sur les configurations permises par la cible de sécurité [ST].

L'évaluation de la partie formelle (ADV_SPM.1) ne couvrent pas l'ensemble complet des fonctions de sécurité pour la cible d'évaluation comme défini dans la cible de sécurité [ST]. Mais le périmètre est conforme à celui spécifié dans l'interprétation [JIL_SPM_CC2022] pour la transition CC:2022.

3 L'évaluation

3.1 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 répondre aux spécificités des cartes à puce et dispositifs similaires, 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).

3.2 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** ».

3.3 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 [ANA_CRY].

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.

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.

Le produit comporte un générateur d'aléa. Il a été analysé conformément à la méthode d'évaluation [AIS20/31] ainsi que les dispositions décrites dans la note d'application [NOTE-24].

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2024/26-R01 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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 3.

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].

4.3 Reconnaissance du certificat

4.3.1 *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[1], 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 :

4.3.2 *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[2] , 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 :

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

[2] 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 Lite of S3SSE2A*, référence Lumbee3R1_ST_Ver1.8, version 1.8, 28 juillet 2025. 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 S3SSE2A*, référence ST_LITE_Ver1.1, version 1.1, 28 juillet 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) – LUMBEE3-R1*, référence LETI.CESTI.LUM3R1.FULL.001, version 1.2, 27 août 2025. 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) – LUMBEE3-R1*, référence LETI.CESTI.LUM3R1.COMPO.001, version 1.2, 27 août 2025.
[ANA_CRY]	*Analysis of cryptographic mechanisms LUMBEE3-R1*, référence LETI.CESTI.LUM3-R1.RT.001, version 1.0, 30 juin 2025.
[GUIDES]	- *S3SSE2A HW DTRNG FRO M and DTRNG FRO M Library Application Note*, référence, version 1.0, 7 décembre 2023 ; - *CRYSTALS ML-DSA (Module Lattice based Digital signature algorithm) Library v1.15 API Manual*, version 1.10, 2 juin 2025 ; - *S3SSE2A User's Manual*, référence S3SSE2A_UM_REV1.0, version 1.0, 8 avril 2025 ; - *Security Application Note For S3SSE2A*, référence SAN_S3SSE2A, version 0.3, 9 mai 2025 ; - *S3SSE2A Chip Delivery Specification (H/W Revision : 0)*, version 1.01, 9 mai 2025 ; - *S3SSE2A Boot Loader Specification*, version 0.5, 10 mai 2025 ; - *S3SSE2A System API Application Note*, version 1.0, 22 mars 2023 ; - *SC300 Reference Manual*, version 0.0, 12 mai 2014 ; - *Cryptographic Mechanisms For S3SSE2A,* version 0.2, 26 mars 2025.
[SITES]	La liste des sites est disponible dans le tableau au chapitre 1.2.3 « TOE Life cycle » de la cible de sécurité.
[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, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4.
[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]	*Information technology — Security techniques — Evaluation criteria for IT security* - *Part 1: Introduction and general model :* ISO/IEC 15408-1:2022 ; - *Part 2: Security functional components:* ISO/IEC 15408-2:2022 ; - *Part 3: Security Assurance components:* ISO/IEC 15408-3:2022 ; - *Part 4: Framework for the specification of evaluation methods and activities*: ISO/IEC 15408-4:2022 ; - *Part 5: Pre-defined packages of security requirements*: ISO/IEC 15408-5:2022. Equivalent à la version CCRA: *Common Criteria for Information Technology Security* Evaluation, version CC:2022, révision 1, parties 1 à 5, références CCMB-2022-11-001 à CCMB-2022-11-005.
[CEM]	*Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 18045:2022* Equivalent à la version CCRA: *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* version *CC:2022,* révision 1, référence CCMB-2022-11-006.
[CC-Errata]	*Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)*, référence 002, version 1.1, 22 juillet 2024.
[CC2022-Transition]	*Transition policy to CC:2022 and CEM:2022*, reference CCMC-2023-04-001, 20 avril 2023.
[JIWG IC] *	*Mandatory Technical Document – The Application of CC to Integrated Circuits*, version 4.0, avril 2024.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2.1, février 2024.

[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.
[AIS20/31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).
[NOTE-24]	Note d'application – Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, référence ANSSI-CC-NOTE-24, version en vigueur.

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