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 EUCC-ANSSI-2025-03-01

ST54J / ST54K (A07)

Paris, le 31 mars 2025

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

Vincent STRUBEL

[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

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).

Ce rapport est conforme à [EUCC].

Les procédures de certification sont disponibles sur le site Internet www.cyber.gouv.fr.

TABLE DES MATIERES

1 Résumé

Référence du rapport de certification **EUCC-ANSSI-2025-03-01**
Nom du produit **ST54J / ST54K**
Référence/version du produit **A07**
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"* *"Loader dedicated for usage in Secured Environment only"* *"Loader dedicated for usage by authorized users only"*
Critères d'évaluation et version **ISO/IEC 15408-1:2009, 15408-2:2008 15408-3:2008** **(Critères Communs version 3.1 révision 5)** **ISO/IEC 18045:2008** **(CEM version 3.1 révision 5)**
Niveau d'évaluation **Elevé / EAL5 augmenté** ALC_DVS.2, ALC_FLR.2, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report PEACOCK A07 Project* référence PEACOCK_A07_2024_ETR_v1.1 version 1.1 11 février 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Résumé des menaces *Inherent Information Leakage* *Physical Probing* *Malfunction due to Environmental Stress* *Physical Manipulation* *Forced Information Leakage*

Abuse of Functionality *Deficiency of Random Numbers* *Masquerade the TOE* *Memory Access Violation* *Diffusion of open samples* (voir chapitre 3 [ST])
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 **STMICROELECTRONICS** 190 Avenue Celestin Coq, 13106 Rousset, France
Commanditaire **STMICROELECTRONICS** 190 Avenue Celestin Coq, 13106 Rousset, France
Centre d'évaluation **SERMA SAFETY & SECURITY** 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
Marque EUCC CC Critères communs CERTIFICATION DE CYBERSÉCURITÉ ÉLEVÉ SUBSTANTIEL BASIQUE Niveau AVA_VAN5 EUCC-ANSSI-2025-03-01
Accords de reconnaissance applicables CCRA Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.2

2 Le produit

2.1 Présentation du produit

Le produit évalué est « ST54J / ST54K, A07 » développé par STMICROELECTRONICS.

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* « *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 :

- *Two instances of the SecurCore® SC300™ CPU connected in Lockstep mode ;*
- *Die integrity ;*
- *Monitoring of environmental parameters ;*
- *Protection mechanisms against faults ;*
- *AIS20/AIS31 class PTG.2 compliant True Random Number Generator ;*
- *Memory Management Unit ;*
- *CRC calculation block ;*
- *Optional hardware Security enhanced DES accelerator ;*
- *Optional hardware Security AES accelerator ;*
- *Optional NExt Step CRYPTography accelerator (Nescrypt).*

Ces services de sécurité sont définis dans la cible de sécurité [ST] au chapitre 1.5 « *TOE overview* ».

2.2.3 *Architecture*

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité [ST] au chapitre 1.6 *« TOE description »*.

2.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit ne contient pas de composants développés par un tiers.

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la la Table 1 « TOE components » du chapitre 1.4 « *TOE identification* » de la cible de sécurité [ST].

Eléments de configuration			Données d'identification lues
Identification du microcontrôleur	*IC Maskset name*		K520B
	IC Version	*ST54J*	C et D
		ST54K	D
	Master identification number		01CAh
Identification des logiciels embarqués	*Firmware version*		3.1.2
	OST Version		09.01

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES]. Il est également possible de faire appel à une fonction en ligne de commande qui renvoie les informations de configuration du produit.

2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit dans la cible de sécurité [ST] au chapitre 1.7 *« TOE life cycle »*. Il est conforme au cycle de vie de sept phases décrit dans [PP0084].

Le produit a été développé sur les sites mentionnés dans la table 15 de la cible [ST]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

2.2.6 *Configuration évaluée*

Le certificat porte sur le microcontrôleur identifié dans la cible de sécurité [ST] au chapitre 1.4 *« TOE identification »*, dans ses configurations permises par les [GUIDES]. Les différentes variantes présentées en table 2 de la cible de sécurité sont toutes couvertes par le certificat. Au regard du cycle de vie, le certificat porte sur le produit livré à l'issue de la phase 3 comme de la phase 4.

2.3 Contacts du produit

Les informations en matière de cybersécurité du produit sont disponibles ici :

- ST54J : ST54J - NFC controller and Secure Element single die - STMicroelectronics
- ST54K : ST54K - NFC controller and Secure Element single die and a UWB secure, fine-ranging subsystem host - STMicroelectronics

Le développeur peut être contacté via cette adresse : psirt@st.com.

La procédure complète de signalement d'une vulnérabilité est disponible sur le lien suivant : PSIRT - STMicroelectronics.

Les informations sur l'Autorité nationale de certification de cybersécurité en France sont disponibles ici https://cyber.gouv.fr/cybersecurity-act.

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 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 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, 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 [RTE].

Cette analyse a identifié des non-conformités par rapport aux référentiels [ANSSI Crypto] et [SOG-IS 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 aux référentiels [ANSSI Crypto] et [SOG-IS Crypto], pour les mécanismes cryptographiques qui le permettent.

3.4 Analyse du générateur d'aléa

Le produit comporte un générateur physique d'aléa 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 aux référentiels [ANSSI Crypto] et [SOG-IS 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 les documents [ANSSI Crypto] et [SOG-IS 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 a aussi été analysé conformément à la méthode d'évaluation [AIS20/31] et suivant 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 et à [EUCC].

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 EUCC-ANSSI-2025-03-01 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.

Le certificat est délivré sous accréditation du COFRAC.

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]. Notamment :

- Les restrictions d'utilisation : chapitre 2 « *Security recommendations versus attack classes* » du guide « *Application note ST54J platform SE subsystem Security guidance* ».
- Pour les restrictions de déploiement et d'environnement, l'utilisateur devra se référer et bien suivre les recommandations présentes dans le guide « *ST54J_SE firmware V3 - User manual* ».

4.4 Reconnaissance du certificat

4.4.1 *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[1] , 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 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 : - *ST54J / ST54K A07 Security Target*, référence SMD_ST54J_ST_17_001, version A07.1, 14 novembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ST54J / ST54K A07 Security Target for composition*, référence SMD_ST54J_ST_17_002, version A07.1, novembre 2024.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report PEACOCK A07 Project*, référence PEACOCK_A07_2024_ETR_v1.1, version 1.1, 11 février 2025. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report for Composition PEACOCK A07 Project*, référence PEACOCK_A07_2024_Lite_ETR_v1.1, version 1.1, 11 février 2025.
[CONF]	Liste de configuration du produit : - *ST54J A07 – HW Rev C – CONFIGURATION LIST*, référence SMD_ST54J_A07_CFGL_24_001, version 1.0, 3 décembre 2024. - *ST54J / ST54K A07 – HW Rev D – CONFIGURATION LIST*, référence SMD_ST54J-K_A07_CFGL_24_002, version 1.0, 3 décembre 2024.
[GUIDES]	*ST54J ST54K NFC controller and secure element system in package Datasheet*, référence DS_ST54J, version 13, 21 mai 2024. *ST54J platform SE subsystem OS developer's guide - user manual*, référence UM_ST54J_SE, version 8, février 2020. *Application note ST54J platform SE subsystem Security guidance*, référence AN_SECU_ST54J_SE, version 4, 17 octobre 2024. *ST54J_SE firmware V3 - User manual*, référence UM_ST54J_SE_FWv3, version 8, mai 2020. *ARM® SC300 r0p1 Technical Reference Manual*, référence ARM_DDI_0447, version A, juin 2009. *ARM® Cortex M3 r2p0 Technical Reference Manual*, référence ARM DDI 0337F3c, version F3c, janvier 2008. *ARM® SecurCore SC300 Errata*, référence PR326-PRDC-009983, version 11, février 2015. *ST54J_SE subsystem - AIS31 compliant random number - User manual*, référence UM_ST54J_SE_AIS31, version 1, mars 2018. *ST54J_SE_Errata*, référence ES_ST54J_SE, version 1, juin 2020.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - STM_2024_ALC_GEN_v1.1 ;

	- STM_2023_RST_CMP_STAR_v1.2 ; - STM_2022_CRL_STAR_v1.1 ; - STM_2022_AMK1_STAR_v1.0 ; - STM_2022_GNB_STAR_v1.2 ; - STM_2022_RNS_STAR_v1.1 ; - STM_2023_SOP_STAR_v1.0 ; - STM_2024_ST Ljubljana_STAR_v1.0 ; - STM_2022_CAT-PAL_STAR_v1.1 ; - STM_2023_TPY-AMK6_STAR_v1.0 ; - STM_2023_LYG_STAR_v1.0 ; - STM_2022_TNS_STAR_v1.0 ; - STM_2023_Pantos_STAR_v1.0 ; - STM_2023_ATT3_STAR_v1.2 ; - STM_2023_Winstek_STAR_v1.0 ; - STM_2023_DNP_STAR_v1.1 ; - STM_2022_DPE_STAR_v1.1.
[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 5.1.
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements.
[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 15408-1:2009 ; - *Part 2: Security functional components:* ISO/IEC 15408-2:2008 ; - *Part 3: Security Assurance components:* ISO/IEC 15408-3:2008 ; - et correctifs techniques associés. Equivalent à la version CCRA: *Common Criteria for Information Technology Security Evaluation* version 3.1, révision *5,* parties 1 à 3, références CCMB-2017-04-001 à CCMB-2017-04-003.
[CEM]	*Information technology — Security techniques — Methodology for IT security evaluation,* ISO/IEC 18045:2008, et correctifs techniques associés. Equivalent à la version CCRA: *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, 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 3.2.1, février 2024.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[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.
[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.3, février 2023.

[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.

* Dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.