



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Certification report EUCC-ANSSI-2025-03-01

**ST54J / ST54K
(A07)**

Paris, the 31/03/2025

COURTESY TRANSLATION



WARNING

This report is intended to provide people who request evaluations with a document to certify the level of security provided by the product under the usage or operating conditions defined in this report for the version which was evaluated. It is also intended to provide potential acquirers of the product with the conditions under which they may use the product to ensure that they meet the conditions for which the product was evaluated and certified; this is why the certification report must be read in conjunction with the evaluated usage and administration guides and with the product's security target which describes the pre-supposed threats, environmental hypotheses and usage conditions so that the user can judge whether the product is suitable for their needs in terms of security objectives.

The certification does not in itself constitute a product recommendation by the Agence nationale de la sécurité des systèmes d'information (ANSSI) and does not guarantee that the certified product is completely free of vulnerabilities that can be exploited.

All correspondence related to this report must be sent to:

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

Reproduction of this document without alteration or cutting is authorized.

FOREWORD

Certification of the security provided by information technology products and systems is governed by amended decree 2002-535 of 18th April 2002. This decree indicates that:

- The *Agence nationale de la sécurité des systèmes d'information* drafts the certification reports. These reports specify the characteristics of the security objectives proposed. They may contain any warnings that their authors consider are worth mentioning for security reasons.
- The certificates awarded by the *directeur général de l'Agence nationale de la sécurité des systèmes d'information* certify that the individual product or system submitted for evaluation meets the specified security characteristics. They also certify that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (article 8).

This report is in compliance with [EUCC].

The certification procedures are available on the website www.cyber.gouv.fr.

TABLE DES MATIERES

1	Summary	5
2	Product	7
2.1	Product presentation	7
2.2	Product description	7
2.2.1	Introduction	7
2.2.2	Security services.....	7
2.2.3	Architecture	8
2.2.4	Product identification	8
2.2.5	Lifecycle.....	8
2.2.6	Evaluated configuration	9
2.3	Product contacts.....	9
3	Evaluation.....	10
3.1	Evaluation reference bases.....	10
3.2	Evaluation work	10
3.3	Analysis of cryptographic mechanisms according to ANSSI technical standards	11
3.4	Random number generator.....	11
4	Certification	12
4.1	Conclusion.....	12
4.2	Usage restrictions.....	12
4.3	Certificate recognition.....	12
4.3.1	International Common Criteria Recognition (CCRA)	12
ANNEXE A.	Documentary references for the product evaluated	14
ANNEXE B.	Certification references	16

1 Summary

Reference of the certification report	
Product name	
Product reference/version	EUCC-ANSSI-2025-03-01
Type of product	ST54J / ST54K
Protection profile compliance	A07 Smart cards and similar devices Security IC Platform Protection Profile certified BSI-CC-PP-0084-2014 (19/02/2014) with Augmentation Packages, version 1.0 with compliance to the packages : "Authentication of the security IC" "Loader dedicated for usage in Secured Environment only" "Loader dedicated for usage by authorized users only"
Evaluation criteria and version	ISO/IEC 15408-1:2009, 15408-2:2008 15408-3:2008 (Critères Communs version 3.1 revision 5) ISO/IEC 18045:2008 High / EAL5 (SEM version 3.1 revision 5) (CEM version 3.1 revision 5)
Evaluation level	ALC_DVS.2, ALC_FLR.2, AVA_VAN.5
Product security features	Evaluation Technical Report PEACOCK A07 Project reference PEACOCK_A07_2024_ETR_v1.1 version 1.1 11/02/2025
Product's Security Features	see 2.2.2 Security services
Threat summary	<i>Inherent Information Leakage</i> <i>Physical Probing</i> <i>Malfunction due to Environmental Stress</i> <i>Physical Manipulation</i> <i>Forced Information Leakage</i>

	<i>Abuse of Functionality</i> <i>Deficiency of Random Numbers</i> <i>Masquerade the TOE</i> <i>Memory Access Violation</i> <i>Diffusion of open samples</i> (voir chapitre 3 [ST])
Product configuration requirements	see 1.1 Usage restrictions
Operating environment assumptions	see 1.1 Usage restrictions
Developer	190 Avenue Celestin Coq, 13106 Rousset, France
Sponsor	STMICROELECTRONICS 190 Avenue Celestin Coq, STMICROELECTRONICS 13106 Rousset, France
Evaluation center (ITSEF)	SERMA SAFETY & SECURITY 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
EUCC mark	CC Critères communs  CERTIFICATION DE CYBERSÉCURITÉ CCRA ELEVÉ SUBSTANTIEL BASIQUE Niveau AVA_VAN5 EUCC-ANSSI-2025-03-01 
Applicable recognition agreements	This certificate is recognized at EAL2 level augmented with CCIR R.2. 

2 Product

2.1 Product presentation

The product evaluated is « ST54J / ST54K, A07 » developed by STMICROELECTRONICS.

The microcontroller on its own is not a product that may be used in its current state. It is intended to host one or more applications. It may be inserted into a plastic support to constitute a smart card. This product has multiple uses (secure identity documents, banking applications, subscription television, transport, health, etc.) depending on the application software embedded in it. These software are not part of this evaluation.

2.2 Product description

2.2.1 Introduction

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operating environment.

This security target complies strictly with the protection profile [PP0084], with:

- « *Authentication of the security IC* » package ;
- « *loader dedicated for usage in secured environment only* » package ;
- « *loader dedicated for usage by authorized users only* » package.

2.2.2 Security services

The main security services provided by the product are:

- *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).*

Those securities services are defined in [ST], section 1.5 « TOE overview ».

2.2.3 Architecture

The product is composed of a hardware part and a software part which are described in [ST] section 1.6 « *TOE description* ».

2.2.4 Product identification

The elements integrated in the product are identified in [CONF].

The certified version of the product does not include component developed by a third party.

The certified version of the product is defined by the following table, detailed in Table 1 « TOE components » of section 1.4 « *TOE identification* » of [ST].

Configuration item			Read data identification
Microcontroller	IC Maskset name		K520B
	IC Version	ST54J	C et D
		ST54K	D
	Master identification number		01CAh
Embedded softwares	Firmware version		3.1.2
	OST Version		09.01

Those items can be verified by reading the registers hosted in the memory identified in [GUIDES]. It is also possible to use a command line function that returns the product configuration information.

2.2.5 Lifecycle

The product lifecycle is described in [ST] section 1.7 « *TOE life cycle* » and is consistent with [PP0084].

The product has been developed on the sites described in the table 15 of [ST]. Reports on site audits carried out under the French scheme, which can be reused without site certification, are listed in [SITES].

2.2.6 Evaluated configuration

The certificate relates to the microcontroller identified in the security target [ST] section 1.4 « *TOE identification* », in the configurations allowed by [GUIDES]. The various configuration possibilities identified in table 2 of [ST] are all included in the certificate.

Regarding the lifecycle, the certificate relates to the product delivered after phase 3 or phase 4.

2.3 Product contacts

- 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

The product's subsystem host - STMicroelectronics

psirt@st.com

PSIRT - STMicroelectronics

The developer can be contacted at this address:

The complete procedure for the vulnerability handling is available here :

<https://cyber.gouv.fr/cybersecurity-act>

Information on France's National Cybersecurity Certification Authority is available here

3 Evaluation

3.1 Evaluation reference bases

The evaluation was carried out in accordance with the Common Criteria [CC], and with the evaluation methodology defined in the manual [CEM].

For assurance components not covered by the [CEM] manual, methods specific to the evaluation center and validated by ANSSI have been used.

To meet the specific requirements of Smart cards and similar devices, the [JIWG IC] and [JIWG AP] guides were applied. Thus, the AVA_VAN level has been determined using the rating scale of the [JIWG AP] guide. As a reminder, this rating scale is more demanding than the one defined by default in the standard [CC] method, used for other product categories (software products, for example).

3.2 Evaluation work

The evaluation technical report [ETR], which was delivered to the ANSSI the day of its finalization, details the work carried out by the evaluation centre and attests that all the evaluation tasks are rated as **"PASS"**.

3.3 Analysis of cryptographic mechanisms according to ANSSI technical standards

The cryptographic mechanisms implemented by the product's security functions (see [ST]) have been analyzed in accordance with procedure [CRY-P-01] and the results recorded in report [ETR].

This analysis identified the following non-conformities with respect to the standard [ANSSI Crypto] and [SOG-IS Crypto]. They were taken into account in the independent vulnerability analysis carried out by the evaluator and did not reveal any exploitable vulnerabilities for the targeted level of attacker.

The user must refer to the [GUIDES] to configure the product in accordance with the [ANSSI Crypto] and [SOG-IS Crypto], for the cryptographic mechanisms that enable it.

3.4 Random number generator

The product includes a physical random number generator that was analyzed in accordance with the [CRY-P-01] procedure.

This analysis did not identify any non-compliance with the [ANSSI Crypto] and [SOG-IS Crypto] standards.

This analysis did not reveal any blocking statistical biases. This does not confirm that the generated data is truly random, but it does ensure that the generator does not suffer from major design flaws. As stated in the [ANSSI Crypto] and [SOG-IS Crypto] documents, it is recalled that, for cryptographic use, the output of a hardware random number generator must undergo cryptographic algorithmic reprocessing, even if the analysis of the physical random number generator did not reveal any weaknesses.

The independent vulnerability analysis conducted by the evaluator did not reveal any exploitable vulnerabilities for the targeted attacker level.

This random generator was also analyzed in accordance with the evaluation method [AIS20/31] and following the provisions described in the application note [NOTE-24].

4 Certification

4.1 Conclusion

The evaluation was carried out according to current rules and standards with the levels of competence and impartiality required for an approved evaluation body. All of the evaluation work carried out enables a certificate to be issued according to decree 2002-535 and to [EUCC].

This certificate attests that the product under evaluation meets the security requirements specified in its security target [ST] for the intended evaluation level (see chapter 1 Summary).

The certificate associated with this report, referenced EUCC-ANSSI-2025-03-01 a has a date of issue identical to the date of signature of this report and is valid for five years from that date.

The certificate is issued under COFRAC accreditation.

4.2 Usage restrictions

This certificate relates to the product specified in chapter 2.2.4 of this report.

This certificate provides an assessment of the product's resistance to attacks, which are highly generic due to the absence of any specific embedded application. Consequently, the security of a complete product built on the microcontroller can only be assessed by an evaluation of the complete product, based on the results of the evaluation mentioned in chapter 3.

The user of the certified product must ensure compliance with the security objectives for the operating environment, as specified in the security target [ST], and follow the recommendations in the guides provided [GUIDES]. In particular :

- Restrictions on use: chapter 2 « *Security recommendations versus attack classes* » from the guide « *Application note ST54J platform SE subsystem Security guidance* ».
- Deployment and environmental requirements: guide « *ST54J_SE firmware V3 - User manual* ».

4.3 Certificate recognition

4.3.1 International Common Criteria Recognition (CCRA)

This certificate is issued under the conditions of the CCRA agreement [CCRA].

The "Common Criteria Recognition Arrangement" enables recognition of the Common Criteria certificates by the signatory countries¹.

Recognition applies up to the assurance components of CC EAL2 level as well as the ALC_FLR family. Certificates recognized under this agreement are issued with the following mark:

¹ The list of signatory countries of the CCRA arrangement is available on the website www.commoncriteriaportal.org.



COURTESY TRANSLATION

ANNEXE A. Documentary references for the product evaluated

[ST]	Security target for the evaluation: - <i>ST54J / ST54K A07 Security Target</i>, reference SMD_ST54J_ST_17_001, version A07.1, 14/11/2024. For publication purposes, the following security target has been provided and validated as part of this evaluation: - <i>ST54J / ST54K A07 Security Target for composition</i>, reference SMD_ST54J_ST_17_002, version A07.1, November 2024.
[ETR]	Evaluation Technical Report : - <i>Evaluation Technical Report PEACOCK A07 Project</i>, référence PEACOCK_A07_2024_ETR_v1.1, version 1.1, 11/02/2025. For the purpose of composition evaluations with this microcontroller, a technical report for composition has been validated: - <i>Evaluation Technical Report for Composition PEACOCK A07 Project</i>, référence PEACOCK_A07_2024_Lite_ETR_v1.1, version 1.1, 11/02/2025.
[CONF]	Configuration list : - <i>ST54J A07 – HW Rev C – CONFIGURATION LIST</i>, référence SMD_ST54J_A07_CFGL_24_001, version 1.0, 3/12/ 2024. - <i>ST54J / ST54K A07 – HW Rev D – CONFIGURATION LIST</i>, reference SMD_ST54J-K_A07_CFGL_24_002, version 1.0, 3/12/2024.
[GUIDES]	<i>ST54J ST54K NFC controller and secure element system in package Datasheet</i>, reference DS_ST54J, version 13, 21 may 2024. <i>ST54J platform SE subsystem OS developer's guide - user manual</i>, reference UM_ST54J_SE, version 8, february 2020. <i>Application note ST54J platform SE subsystem Security guidance</i>, reference AN_SECU_ST54J_SE, version 4, 17 October 2024. <i>ST54J_SE firmware V3 - User manual</i>, reference UM_ST54J_SE_FWv3, version 8, may 2020. <i>ARM® SC300 r0p1 Technical Reference Manual</i>, reference ARM_DDI_0447, version A, June 2009. <i>ARM® Cortex M3 r2p0 Technical Reference Manual</i>, reference ARM DDI 0337F3c, version F3c, January 2008. <i>ARM® SecurCore SC300 Errata</i>, référence PR326-PRDC-009983, version 11, février 2015. <i>ST54J_SE subsystem - AIS31 compliant random number - User manual</i>, référence UM_ST54J_SE_AIS31, version 1, March 2018. <i>ST54J_SE Errata</i>, référence ES_ST54J_SE, version 1, June 2020.
[SITES]	Document analysis and site audit reports for reuse: - 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]	<i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13/01/2014.</i> Certified by BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) - BSI-PP-0084-2014.

ANNEXE B. Certification references

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 procedure of the security provided by information technology products and systems, reference ANSSI-CER-P-01version 5.1.
[EUCC]	European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.
[CRY-P-01]	Methods for carrying out cryptographic analyses, reference ANSSI-CC-CRY-P01, version 4.1.
[CC]	<i>Information technology — Security techniques — Evaluation criteria for IT security</i> - 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 ; - And and associated technical fixes. Equivalent to CCRA version: <i>Common Criteria for Information Technology Security Evaluation</i> version 3.1, révision 5, parties 1 à 3, references CCMB-2017-04-001 à CCMB-2017-04-003.
[CEM]	<i>Information technology — Security techniques — Methodology for IT security evaluation</i>, ISO/IEC 18045:2008, et correctifs techniques associés. Equivalent à la version CCRA: <i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology</i>, version 3.1, revision 5, reference CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, February 2009.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2.1, February 2024.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2/07/2014.
[ANSSI Crypto]	Guide to cryptographic mechanisms: Rules and recommendations concerning the choice and sizing of cryptographic mechanisms, ANSSI-PG-083, version 2.04, January 2020.
[SOG-IS Crypto]	<i>SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms</i> , version 1.3, February 2023.

[AIS20/31]	<i>A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).</i>
[NOTE-24]	Evaluation of random number generators according to AIS20/31 in the French scheme, reference ANSSI-CC-NOTE-24, current version.

* SOG-IS document; under the CCRA recognition agreement, the equivalent CCRA support document applies.