EUCC Certification Report

JSIGN4 on ST31P450 C03 V1.0.4

Sponsor and developer:	***STMicroelectronics S.r.l*** **Zona Industriale Marcianise SUD** **81025 Marcianise (CE)** **Italy**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**EUCC-3110-2026-2500132-01 Certification Report**
Report version:	**1.0**
Project number:	**EUCC-2500132-01**
Author(s):	**Haico Haak, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**31 August 2026**
Number of pages:	**18**
Number of appendices:	**0**

Reproduction of this report is authorised only if reproduced in its entirety.

® TrustCB is a registered trademark. Any use or application requires prior approval by TrustCB.

CONTENTS

Foreword 3

International recognition of the certificate 4

1 Executive Summary 5

2 ICT Product details 7

2.1 Identification of the ICT Product 7
2.2 Contact information related to the evaluation of the ICT Product 7
2.3 Security services and policies 7
2.3.1 Security services 7
2.3.2 Vulnerability management 8
2.3.3 Assurance Continuity policies 8
2.3.4 Lifecycle management processes and production facilities 8
2.3.5 Patch management process 8
2.4 Assumptions and Clarification of Scope 8
2.4.1 Assumptions 8
2.4.2 Clarification of scope 8
2.5 Architectural Information 8
2.6 Supplementary Cybersecurity Information 9

3 Evaluation summary 10

3.1 Identification of used assurance components 10
3.2 EUCC State of the Art documents and Protection Profiles 10
3.3 ICT Product testing 10
3.3.1 Testing approach and depth 10
3.3.2 Independent penetration testing 10
3.3.3 Test configuration 11
3.3.4 Test results 11
3.4 ICT Product evaluation 11
3.4.1 Reused evaluation results 11
3.4.2 Evaluated configuration 11
3.4.3 Assessment against each assurance requirement 11
3.5 Results of the evaluation 13
3.6 Certificate information and scheme label 13
3.7 Comments and Recommendations 13

4 Security Target 15

5 Glossary 15

6 Bibliography 17

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

Reproduction of this report is authorised only if it is reproduced in its entirety.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the JSIGN4 on ST31P450 C03 V1.0.4, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is STMicroelectronics S.r.l located in Marcianise, Italy and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE is a smartcard SW application implementing a Secure Signature-Creation Device with key generation as described in [EN419211-2], [EN419211-4], [EN419211-5] and CIE/CNS application (Italian identity and service citizen card see [CNS]) designed as a Java card applet integrated on STMicroelectronics Java Card platform designed for the STMicroelectronics ST31P450 ICC C03 (ST31P450 Security Integrated Circuit with dedicated software and embedded cryptographic library).

The TOE claims conformance to the following Protection Profiles *[PP]*:

- EN 419211-2:2013, Protection profiles for secure signature creation device – Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
- EN 419211-4:2013, Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, V1.0.1, registered under the reference BSI-CC-PP-0071-2012-MA-01
- EN 419211-5:2013, Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500132-01**, dated 31-08-2026 and with a 5-year validity.

The evaluation of the TOE was performed by SGS Brightsight B.V. located in Delft. The evaluation was completed on 28-08-2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The TOE is stated as a Qualified Signature Creation Device for the purposes of electronic identification and trust services as detailed by [EU-eIDAS]. The evaluation by SGS Brightsight B.V. included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 7 0.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 “Flaw Reporting Procedures” and AVA_VAN.5 (Advanced methodical vulnerability analysis). It also includes the assurance Composite product package as defined in *[CC]*(Part 5).

This assurance level is recognised by article 52 of [CSA] as ‘high’.

Consumers of this ICT Product are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

---

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and/or qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product JSIGN4 on ST31P450 C03 V1.0.4 from STMicroelectronics S.r.l located in Marcianise, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ST31P450 IC	C03
Embedded Software	NESLIB cryptographic library	Version. 6.4.7
Software	CIE/CNS application designed as a Java card applet integrated on STMicroelectronics Java Card platform	1.0.4

Additional requirements for the operational environment of the certified ICT product are described in section 9.2 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	STMicroelectronics S.r.l
Address:	Zona Industriale Marcianise SUD, 81025 Marcianise (CE), Italy
Certified product contact details	laurent.dirusso@st.com

Developer of the certified ICT Product

ICT product developer	STMicroelectronics S.r.l

Identification of CAB

The Certification Assessment Body for this ICT Product is **TrustCB B.V** located in Hoofddorp, The Netherlands.

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

SGS Brightsight in Delft, the Netherlands

Responsible national cybersecurity certification authority

Dutch Authority for Digital Infrastructure (RDI)

2.3 Security services and policies

2.3.1 Security services

The TOE security features can be summarized as follows:

• Cryptographic key generation and secure management

• Secure signature generation with secure management of data to be signed

• Identification and Authentication of trusted users and applications

• Data storage and protection from modification or disclosures

• Secure exchange of sensitive data between the TOE and a trusted applications CGA/SCA

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the JSIGN4 on ST31P450 C03 V1.0.4

Document reference: A public web page accessible from any search engine:

https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 6.4.

2.3.5 Patch management process

Not applicable to this evaluation.

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 9.2 of the *[ST]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [*ST]*.

Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

2.4.2 Clarification of scope

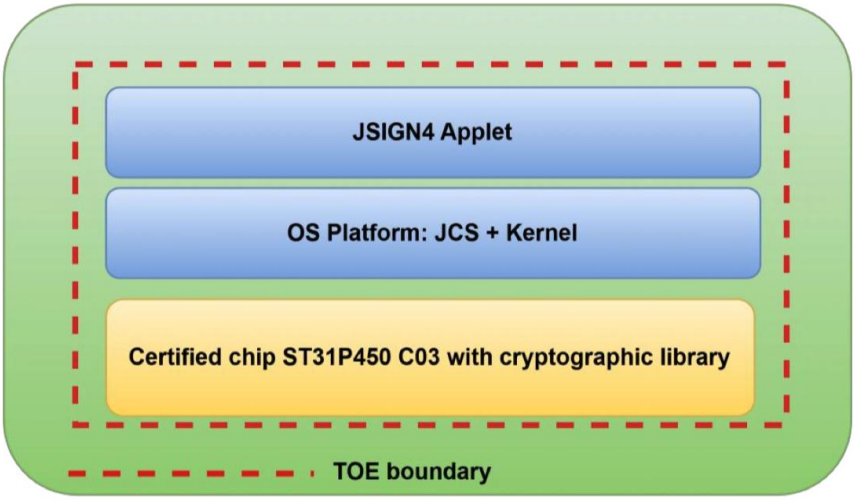
Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Threats addressed by the TOE and the IT environment are presented in Section 8.4 of *[ST]* and include the threats as presented in the *[EN419211-2], [EN419211-4]* and *[EN419211-5]*. No items have been added, removed or modified for the TOE. The assumed level of expertise of the attacker for all identified threats is High.

The Organizational Security Polices (OSPs) are the same as in *[EN419211-2], [EN419211-4]* and *[EN419211-5]*. No OSPs have been added, removed or modified.

2.5 Architectural Information

The Target Of Evaluation (TOE) is a composite TOE which is the Secure Signature Creation Device (SSCD) with key generation (JSIGN4 with OS Platform) and the secure IC STMicroelectronics ST31P450. The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.6 Supplementary Cybersecurity Information

The following website link was provided for the JSIGN4 on ST31P450 C03 V1.0.4 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.st.com/en/secure-mcus/j-sign4.html

This link provides further details and links on:

- Guidance and recommendations to assist end users of the TOE with the secure configuration, installation, deployment, operation and maintenance of the JSIGN4 on ST31P450 C03 V1.0.4 (https://www.st.com/resource/en/security_guidance/sg0066-cyber-security-information-for-certified-products-stmicroelectronics.pdf)
- The period during which the JSIGN4 on ST31P450 C03 V1.0.4 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated as aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the JSIGN4 on ST31P450 C03 V1.0.4. (https://www.st.com/resource/en/security_guidance/sg0066-cyber-security-information-for-certified-products-stmicroelectronics.pdf)
- the online repository listing publicly disclosed vulnerabilities related to the JSIGN4 on ST31P450 C03 V1.0.4 and to any relevant cybersecurity advisories. (https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html)

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the JSIGN4 on ST31P450 C03 V1.0.4:

Identifier	Version
JSIGN4 V1.0.4 on ST31P450 C03 Preparative Procedure	Revision C
JSIGN4 on ST31P450 C03 Operational User Guidance	Revision B

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 4 augmented with ALC_FLR.2 and AVA_VAN.5** and
- **Composition evaluation package (COMP)**,

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents *SotA Documents* were applied as referenced in the Bibliography.

The following Protection Profiles were applied:

EN 419211-2:2013, Protection profiles for secure signature creation device – Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI),

EN 419211-4:2013, Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, V1.0.1, registered under the reference BSI-CC-PP-0071-2012-MA-01 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI),

EN 419211-5:2013, Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI).

3.3 ICT Product testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

3.3.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

3.3.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During the attack oriented analysis the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of (additional) potential vulnerabilities, the analysis of which was performed according to the attack methods in

[SotA_AAPS]. An important source for assurance in this step was the technical report *[HW-ETRfC]* of the underlying platform.

- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities were not exploitable. The potential vulnerabilities were demonstrated to be non-exploitable through penetration testing or were addressed by a guidance update.

The total test effort expended by the evaluators was 4 weeks. During that test campaign 0% of the total time was spent on physical attacks, 0% on overcoming sensors and filters, 25% on perturbation attacks and retrieving keys with FA, 75% side-channel attacks, 0% exploitation of test features, 0% attacks on RNG, 0% software attacks, and 0% on application isolation penetration tests.

3.3.3 Test configuration

The developer tested the TOE in the following configuration

- JSIGN4 on ST31P450 C03 V1.0.4

3.3.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

3.4 ICT Product evaluation

The evaluation was performed referencing ISO/IEC 18045, Common Evaluation Methodology, and the EUCC State of the Art documents listed in section 6 of this report as *SotA* Documents.

Further security evaluation criteria were not applied in this evaluation.

3.4.1 Reused evaluation results

This was a new certification under EUCC.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of two site certificates and Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number JSIGN4 on ST31P450 C03 V1.0.4.

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2

TOE summary specification	ASE.TSS.1
Consistency of Composite product ST	ASE.COMP.1

The [ST] contains all relevant information for this class and the according families according to EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 and the COMP package.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.4
Implementation representation	ADV_IMP.1
TOE design	ADV_TDS.3
Composite design compliance	ADV_COMP.1

Developer Evidence, i.e. implementation representation was provided that enabled the evaluator to ensure that all relevant aspects for this class and the according families according to EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 and the COMP package are met by the TOE.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The guidance documentation for the TOE, as outlined in the *[ST]* is provided that contains all relevant information for this class and the according families according to EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 and the COMP package.

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.4
Delivery	ALC_DEL.1
Development security	ALC_DVS.1
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2
Tools and techniques	ALC_TAT.1
Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1

The TOE Life Cycle is covered by audited sites and Developer Documentation has been provided that contains all relevant information for this class and the according families according to EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 and the COMP package.

ATE

ATE

Coverage	ATE_COV.2
Depth	ATE_DPT.1
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2
Composite functional testing	ATE_COMP.1

The developer provided Test documentation, a test witnessing session was performed and independent testing was performed. The provided information enabled the evaluator to positively assess that the TOE meets this class and the according families according to EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 and the COMP package.

AVA

AVA	
Vulnerability analysis	AVA_VAN.5
Composite vulnerability assessment	AVA_COMP.1

A vulnerability analysis was performed and penetration tests based on the analysis were conducted. No deviation from the expected result was detected. Therefore, the TOE meets this class and the according families according to EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 and the COMP package.

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS]*.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the evaluation results the evaluation lab concluded the JSIGN4 on ST31P450 C03 V1.0.4, to be **CC:2022 R1 Part 2 conformant, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**High**, with **AVA_VAN 5** and to meet the requirements of **EAL 4 augmented with AVA_VAN.5 and ALC_FLR.2** . This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

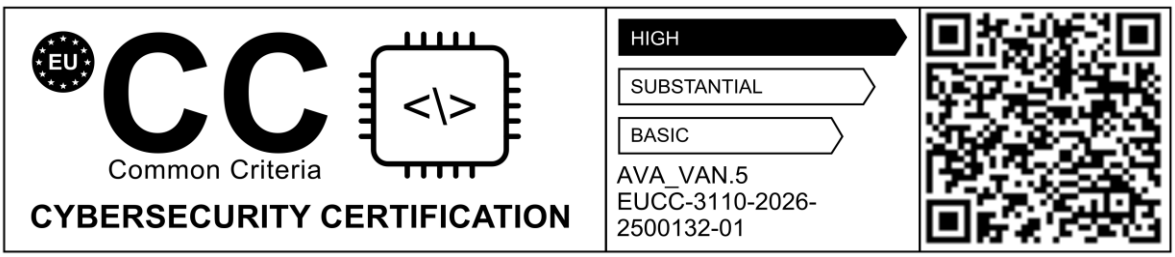
The Security Target claims 'strict' conformance to the Protection Profiles *[EN419211-2], [EN419211-4]* and *[EN419211-5]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500132-01

Date of issuance: 31-08-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks,

depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a “high attack potential”, appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

4 Security Target

The certification references the following security target:

JSIGN4 on ST31P450 C03 Security Target, Rev. H, 28 August 2026 *[ST]*.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AC	Access Conditions
BSO	Base Security Object
CC	Common Criteria
CGA	Certificate Generation Application
CNS	Carta Nazionale Servizi (National Services Card for Italian citizen)
CRT	Chinese Remainder Theorem
CSP	Certification Service Provider
DES	Data Encryption Standard
DF	Directory file
DTBS	Data to be signed
DTBSR	Data to be signed representation
EAL	Evaluation Assurance Level
HPC	Health Professional Card
IC	Integrated Circuit
IFD	Interface Device, i.e. the smartcard reader
IT	Information Technology
JCS	Java Card System
MAC	Message Authentication Code
MAP	Modular Arithmetic Processor
MUTKEY	Cryptographic key used for mutual authentication between the TOE and an external application/device
OS	Operating System
RAD	Reference Authentication Data
RAD_A	Reference Authentication Data stored by the TOE and used to verify the claimed identity of the administrator
RAD_S	Reference Authentication Data stored by the TOE and used to verify the claimed identity of the signatory
SC	Smartcard
SCA	Signature Creation Application
SCD	Signature Creation Data
SDO	Signed Data Object

SF	Security Function
SFP	Security Function Policy
SM	Secure Messaging
ST	Security Target
STM	STMicroelectronics
SVD	Signature Verification Data
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VAD	Verification Authentication Data

6 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[CC2022_TP]	CCMC-2023-04-001, Transition Policy to CC:2022 and CEM:2022, 20 April 2023
[DEV_DOCS]	JSIGN4 V1.0.4 on ST31P450 C03 Preparative Procedure, Revision C, 27 April 2026
	JSIGN4 on ST31P450 C03 Operational User Guidance, Revision B, 27 April 2026
	Configuration Item List, 04 July 2025
[eIDAS-REP]	Assessment Reporting Sheet eIDAS STM JSIGN4 on ST31P450 C03, 26-RPT-676, Version 2.0, 22 July 2026
[CNS]	CNS – Carta Nazionale dei Servizi – Functional Specification V1.1.6, 02 April 2011
[EN419211-2]	EN 419211-2:2013, Protection profiles for secure signature creation device – Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
[EN419211-4]	EN 419211-4:2013, Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, V1.0.1, registered under the reference BSI-CC-PP-0071-2012-MA-01
[EN419211-5]	EN 419211-5:2013, Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01
[ETR]	Evaluation Technical Report "JSIGN4 v1.0.4 on ST31P450 C03"– EAL4+, 26-RPT-294, Version 4.0, 28 August 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
	REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[HW-CERT]	Rapport de certification / Certification report EUCC-3090-2025-11-09 ST31P450 including optional cryptographic library NESLIB (C03), 10/12/2025
[HW-ETRfC]	Evaluation Technical Report for composite evaluation, MANDALA C03 REEVALUATION, MANDALA_C03_RE_2025_ETRLite, Version 2.0, 2025-11-13
[HW-ST]	ST31P450 C03 including optional cryptographic library NESLIB Security Target for composition Common Criteria for IT security evaluation, SMD_ST31P450_ST_19_002 Rev C03.2, September 2025
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA_COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation and certification for CC: 2022 Version 1, February 2025
[SotA_QSCD]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices according to eIDAS Regulation (EU) 910/2014, as amended by Regulation (EU) 2024/1183. Version 1, February 2025
[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023
[SotA_STAR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, STAR methodology, version 1, February 2025
[SotA_CRYPTO]	EUCC SCHEME, GUIDELINES ON CRYPTOGRAPHY, Agreed Cryptographic Mechanisms, Version 2, May 2025
[ST]	JSIGN4 on ST31P450 C03 Security Target, Rev. H, 28 August 2026
[ST-lite]	JSIGN4 on ST31P450 C03 Security Target Lite, Rev. D, 28 August 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2
	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)