Certification Report

JSIGN4 V1.0.4

Sponsor and developer:	***ST Microelectronics 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:	**NSCIB-CC-0434407-CR**
Report version:	**2**
Project number:	**0434407**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**18 March 2022**
Number of pages:	**11**
Number of appendices:	**0**

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

Version 2021-06

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) 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 (site) security target is a requirements specification document that defines the scope of the evaluation activities.

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

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

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of 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.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the JSIGN4 V1.0.4. The developer of the JSIGN4 V1.0.4 is ST Microelectronics S.r.l located in Marcianise, Italy and they also act as the sponsor of the evaluation and certification A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a smartcard SW application implementing a Secure Signature-Creation Device with key generation as described in *[EN 419211-2]*, *[EN 419211-4]*, *[EN 419211-5]* 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 B04 (ST31P450 Security Integrated Circuit with dedicated software and embedded cryptographic library).

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2 March 2022 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the JSIGN4 V1.0.4, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the JSIGN4 V1.0.4 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.

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 AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

Version 2 of the Certification Report was generated to address an editorial item in the report.

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

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the JSIGN4 V1.0.4 from ST Microelectronics S.r.l located in Marcianise, Italy.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Hardware	ST31P450 ICC	B04
	NESLIB cryptographic library	6.4.7
Software	CIE/CNS application designed as a Java card applet integrated on STMicroelectronics Java Card platform	1.0.4

To ensure secure usage a set of guidance documents is provided, together with the JSIGN4 V1.0.4. For details, see section 2.5 “Documentation” of this report.

The ST31P450 ICC B04 identified in *[HW-MAINT]* is the same version as the one mentioned in the IC certificate *[HW-CERT]* which was confirmed to be identical for the scope of the composite TOE when applying the updated guidance in *[SUR]*.

2.2 *Security Policy*

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 *Assumptions and Clarification of Scope*

2.3.1 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]* (section 11.2 in *[ST-Lite]*).

2.3.2 Clarification of scope

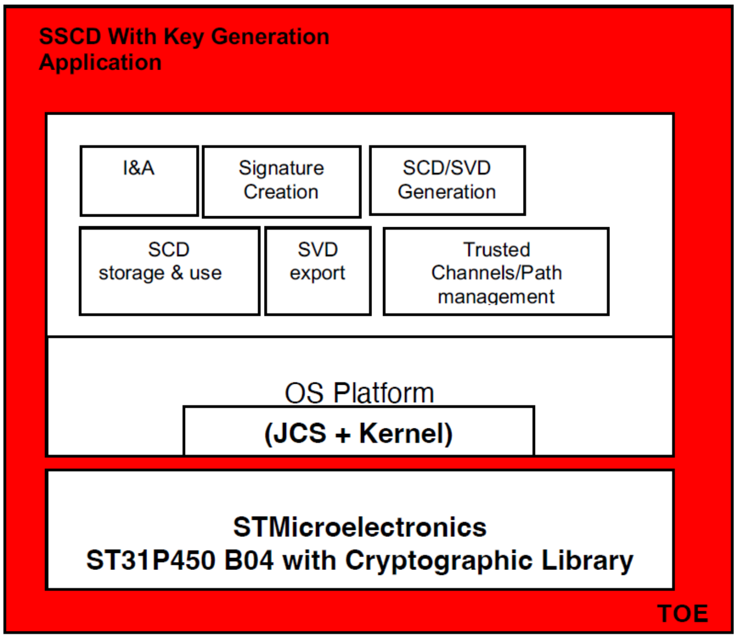
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 *Architectural Information*

The TOE is the composition of an SW application with the secure IC STMicroelectronics ST31P450 ICC B04.

The TOE is a smartcard SW application implementing a SCD with key generation as described in *[EN 419211-2]*, *[EN 419211-4]*, *[EN 419211-5]* 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 B04 (ST31P450 Security Integrated Circuit with dedicated software and embedded cryptographic library).

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
JSIGN4 - Operational User Guidance	Revision B
JSIGN4 - Preparative Procedure	Revision C

2.6 IT 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.

2.6.1 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.

2.6.2 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 *[JIL-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 5 weeks. During that test campaign, 40% of the total time was spent on Perturbation attacks and 60% on side-channel testing.

2.6.3 Test configuration

The developer tested the TOE in the following configuration

- JSIGN4 v1.0.4
- JSIGN4 v1.0.3

The evaluator assessed the differences between the two different versions and has confirmed these where functional bug fixes with no security impact. The results of the testing performed on TOE version 1.0.3 applies to TOE version 1.0.4 and thus the security functionality was demonstrated to be identical.

2.6.4 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.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of one Site Technical Audit Reuse report.

2.8 Evaluated Configuration

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

2.9 Evaluation Results

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

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

Based on the above evaluation results the evaluation lab concluded the JSIGN4 V1.0.4, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5**. 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]*, [EN 419211-4] and *[EN 419211-5]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” 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: NESLIB cryptographic library 6.4.7.

3 Security Target

The JSIGN4 Security Target, Revision F, 17 February 2022 *[ST]* is included here by reference.

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

4 Definitions

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

CGA	Certificate Generation Application
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
SCA	Signature Creation Application
SCD	Signature Creation Device
TOE	Target of Evaluation

5 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, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[CNS]	Carta Nazionale dei Servizi functional Specification, Version 1.1.6
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[EN419211-2]	EN 419 211-2:2013, 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 419 211-4:2013, Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0071-2012-MA-01
[EN419211-5]	EN 419 211-5:2013 Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, version 1.01, registered under the reference BSI-CC-PP-0072-2012-MA-01
[ETR]	Evaluation Technical Report “JSIGN4 v1.0.4” – EAL4+, 21-RPT-943, Version 3.0, 20 February 2022
[HW-CERT]	Rapport de certification ANSSI-CC-2020/05 ST31P450 B02 including optional cryptographic library Neslib version 6.4.7 and optional technology MIFARE Plus® EV1 version 1.1.2, 18 February 2020
[HW-ETRfC]	THALES evaluation Technical Report for composite evaluation Project: MANDALA with library Surveillance, Version 2.0, January 2022
[HW-MAINT]	Rapport de maintenance ANSSI-CC-2020/05-M01, ST31P450 B04 including optional cryptographic library NESLIB version 6.4.7 and optional technology MIFARE Plus® EV1 version 1.1.2, 02 February 2022
[HW-ST]	ST31P450 B04 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1 Security Target for composition, SMD_ST31P450_ST_19_002, Rev B04.1, August 2021
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	JSIGN4 Security Target, Revision F, 17 February 2022
[ST-lite]	JSIGN4 Security Target Lite, Revision E, 17 February 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[SUR]	Rapport de surveillance ANSSI-CC-2020/05-S02, 2 February 2022

(This is the end of this report.)