TÜV Rheinland Nederland B.V.

Certification Report

JSIGN3 V1.1.4

Sponsor and developer:	**ST Microelectronics S.r.l** **Z.I. Marcianise SUD** **81025 Marcianise** **Italy**
Evaluation facility:	**Brightsight** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0122197-CR**
Report version:	**1**
Project number:	**0122197**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**29 June 2020**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 license 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, in order 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 authorized provided the report is reproduced in its entirety.

TÜVRheinland®
Precisely Right.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

eIDAS-Regulation

TÜV Rheinland Nederland B.V., operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 *[EU-REG]*.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the JSIGN3 V1.1.4. The developer of the JSIGN3 V1.1.4 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 [PP-2], [PP-4], [PP-5] and CIE/CNS application (Italian identity and service citizen card, cf. [CNS]) designed as a Java card applet integrated on STMicroelectronics Java Card platform designed for the STMicroelectronics ST31G480 ICC (ST31G480 Security Integrated Circuit with dedicated software and embedded cryptographic library).

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 29 May 2020 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 JSIGN3 V1.1.4, 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 JSIGN3 V1.1.4 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 provides 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]*.

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 meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014. The product meets the requirements defined in [EU-REG] article 29 and article 39 and thus is a QSCD in the sense of [EU-REG]. It will be listed on the NSCIB Certified Products list and will be notified to the European Commission (eIDAS). It should be noted that the certification results only apply to the specific version of the product as evaluated.

---

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

2   Certification Results

2.1   Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the JSIGN3 V1.1.4 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	ST31G480 IC	D01
	NESLIB cryptographic library	6.2.1
Software	CIE/CNS application designed as a Java card applet integrated on STMicroelectronics Java Card platform	1.1.4

To ensure secure usage a set of guidance documents is provided together with the JSIGN3 V1.1.4. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the [ST], chapter 6.5

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 the users.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 9.2 of the *[ST]*.

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 ST31G480.

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 JCSJava Card platform designed for the STMicroelectronics ST31G480 ICC (ST31G480 Security Integrated Circuit with dedicated software and embedded cryptographic library).
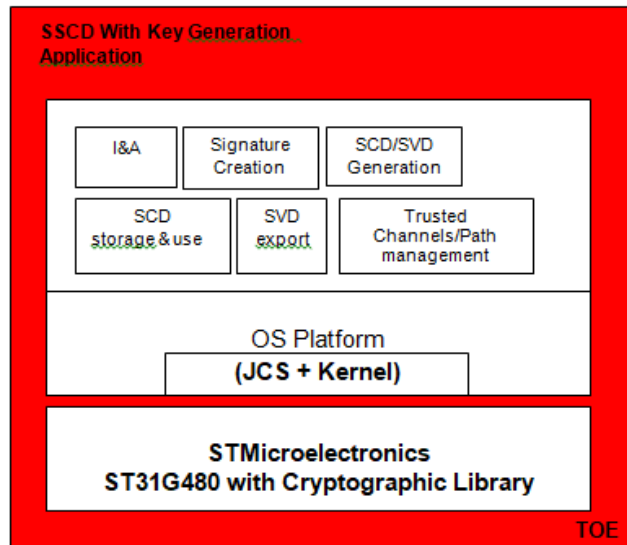
2.5 Documentation

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

Identifier	Version
JSIGN3 Operational User Guidance	Revision K
JSIGN3 Preparative Procedures	Revision D

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

The underlying hardware and crypto-library test results are extendable to composite evaluations, as 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 has provided samples and a test environment. The evaluators have 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:

1. 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.
2. For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional)

potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AP]. An important source for assurance in this step is the technical report [ETRfC-HW] of the underlying platform.

3. All potential vulnerabilities are 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 are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

In total five penetration tests were performed, comprising of two perturbation attacks and three side-channel attacks.

2.6.3 Test Configuration

The TOE was tested in the following configurations:

- JSIGN3 v1.1.4.

2.6.4 Testing 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.

For composite evaluations, please consult the [ETRfC] for details

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 1 Site Technical Audit Re-use report approaches.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number JSIGN3 V1.1.4.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a 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 JSIGN3 V1.1.4, 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 *[PP2] [PP4] [PP5]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 version 6.2.1

3   Security Target

The [ST] JSIGN3 Security Target, revision I, 18-5-2020 is included here by reference.

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

4   Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
SM	Secure Messaging
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.

[ETR]   Evaluation Technical Report JSIGN3 V1.1.4, Evaluation Technical Report "STM JSIGN3 V1.1.4" – EAL4+, version 1.0, 20 May 2020.

[EU-REG]   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

[HW-CERT]   Rapport de certification ANSSI-CC-2019/12

[HW-ETRfC]   ETR for composition ST31G480, Revision 1.3

[HW-ST]   ST31G480 D01 including optional cryptographic library NESLIB, and optional technologies MIFARE® DESFire® EV1 and MIFARE Plus® X Security Target for composition Rev D01.3

[NSCIB]   Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[PP2]   EN 419211-2:2013, Protection Profiles for secure signature creation device - Part 2: Device with key Generation, 2013.

[PP4]   EN 419211-4, Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted channel to certificate generation application, 2013.

[PP5]   EN 419211-5, Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application, 2013

[ST]   [ST] JSIGN3 Security Target, revision I, 18-5-2020.

[ST-SAN]   JSIGN3 Security Target Lite Rev. C 15-May-2020

[CNS]   Carta Nazionale dei Servizi. Functional Specification, Version 1.1.6

(This is the end of this report).