Version 2021-06

Certification Report

TRISS Trust Remote InfoCert Signing Server version 1.0.2

Sponsor and developer:	***InfoCert S.p.A.*** **Piazza Sallustio 9** **00187 Rome** **Italy**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0490158-CR**
Report version:	**2**
Project number:	**0490158**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**30 June 2022**
Number of pages:	**12**
Number of appendices:	**0**

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

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 TRISS Trust Remote InfoCert Signing Server version 1.0.2. The developer of the TRISS Trust Remote InfoCert Signing Server version 1.0.2 is InfoCert S.p.A. located in Rome, 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 combination of software and hardware components defined as Signature Activation Module (SAM). The SAM implements the Signature Activation Protocol (SAP), and it uses the Signature Activation Data (SAD) and Authorisation Data to activate the signing key to be used in the Cryptographic Module. The hardware and firmware are not part of the TOE and is considered to be part of the TOE environment.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 30 June 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 TRISS Trust Remote InfoCert Signing Server version 1.0.2, 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 TRISS Trust Remote InfoCert Signing Server version 1.0.2 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.

[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 TRISS Trust Remote InfoCert Signing Server version 1.0.2 from InfoCert S.p.A. located in Rome, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	TRISS Trust Remote InfoCert Signing Server	V1.0.2

To ensure secure usage a set of guidance documents is provided, together with the TRISS Trust Remote InfoCert Signing Server version 1.0.2. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE has the following security features:

- Operator management:
    - Privileged Users can create other Privileged Users.
- System management
    - Privileged Users can handle system configuration.
- Signer management covers:
    - Privileged Users can create Signers
    - Privileged Users set up the indirect authentication scheme that is assigned to all Signers.
    - Privileged Users or Signers can generate signing keys and Signature Verification Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a Signer. Signer can generate signing keys only for him/herself.
    - Privileged Users or Signers can disable a signing key identifier to be used by a Signer. Signer can disable the own signing key identifier.
- Signature operations
    - Signers can supply a DTBS/R(s) to be signed, Privileged User can’t.
    - The link between Signer authentication, DTBS/R(s) and signing key identifier is handled by the Signature Activation Data (SAD). The SSA securely exchange the SAD with the TOE by using the Signature Activation Protocol (SAP). The following actions are performed within the TOE:
        - The SAD is verified in integrity.
        - The SAD is verified that it binds together the Signer authentication, the DTBS/R(s) and the signing key identifier.
        - The Signer identified in the SAD is authenticated by using indirect authentication scheme only.
        - It is verified that the DTBS/R(s) used for signature operations is bound to the SAD.
        - It is verified that the signing key identifier is assigned to the Signer.
        - The TOE uses Authorisation Data to activate the signing key within the Cryptographic Module.
        - The TOE uses its Cryptographic Module services to create signatures.

- The TOE generates audit records for all security-related events and relies on the SSA to store and provide access control for the records.

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 6.2 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

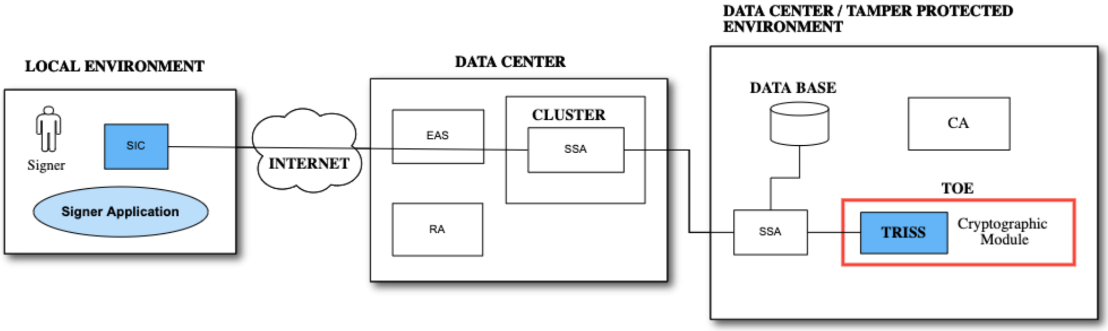

Figure 1 - Logical architecture of the TOE.

The TOE consists of a software application deployed within the tamper protected part of the Cryptographic Module, in a dedicated tamper-protected environment. The local nature of the communication between the software application and the Cryptographic Module within the same physically protected environment ensures integrity and confidentiality protection of the exchanged data, as well as mutual authentication of the communicating IT entities.

Together the TRISS application and the Cryptographic Module are a QSCD (the TOE). In Figure 1, the TOE perimeter is highlighted in red colour. It includes both the Cryptographic Module and the TRISS software application running inside its CPU, and the intended operational environment.

2.5 Documentation

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

Identifier	Version
TRISS AGD_PRE, 31-03-2022	V2.1
TRISS AGD_OPE, 31-03-2022	V2.1

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

In this evaluation, a methodical vulnerability is executed to create fair coverage, by asking security questions inspired by generic weaknesses separately for all security implementations of the TOE. This analysis led to four potential vulnerabilities, which were further analysed.

Around 60 possible vulnerabilities were identified by using the following classifications:

- (ACCESS) Accessibility, which includes:
    - Access Control (proper verification of the privileges of each role)
    - Authentication (proper role determination based on authentication data)
    - Privilege (Proper privileges management)
- (CHANNEL) Channel (secure communication with other trusted parties)
- (CRYPT) Cryptography (crypto usage to protect the TOE and as service)
- (ENTRYPOINT) Entry Points (unexpected entry points that could lead to exposure of confidential information)
- (INPUT) Exception Management (Does the TOE react properly on exceptional inputs/conditions) and Tainted input (corrupted input)
- (LEAK) Information Leak (No confidential information leakage)
- (MALWARE) Malware (no code execution without integrity check possible)
- (MEMORIES) Memories, which includes:
    - Memory Access (proper memory management that is robust against logical anomalies)
    - Memory Management (Proper memory allocation/de-allocation)
    - Resource Management (Proper data handling)
- (CODE) Coding, which includes:
    - Implementation (proper coding rules and implementation of it)
    - Compiler (Compiler does not remove security features)
    - Unused entities (No unexpected usage of dead code)
    - Risky Values (Proper calculation security values)
- (DESIGN) Design and Architecture (Sound architecture of the building blocks)
- (RANDOM) Predictability (proper RNG usage with the required entropy)
- (COMMANDFLOW) Command flow, which includes:
    - Synchronization (Secure TOE behaviour when expected commands order is not followed)
    - Path Resolution (proper data flow)

The applicability of each possible vulnerability are assessed, using design argumentation, developer the evaluator testing or code review. Possible vulnerabilities that require extra attention was considered potential vulnerabilities.

2.6.2 Independent penetration testing

All Automatic developer tests were selected to be repeated. Three of the five Manual developer Tests where selected to be repeated.

The total test effort expended by the evaluators was nine days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE configuration used for testing was TRISS Trust Remote InfoCert Signing Server version 1.0.2.

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

Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number TRISS Trust Remote InfoCert Signing Server version 1.0.2. The TOE user must verify that the SHA-256 fingerprint of the delivered TOE matches the following:

1a7e91b4d70bbe968181cd7a8132cf9931743c1b0d4434883cad9bbe3628181a

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the sites *[STAR_DevCenter] and [STAR_DataCenter]* [2].

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

Based on the above evaluation results the evaluation lab concluded the TRISS Trust Remote InfoCert Signing Server version 1.0.2, 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 Profile *[PP]*.

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.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

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).

3 Security Target

The Signature Activation Module Trust Remote InfoCert Signing Server – TRISS Security Target, Version 2.1, 31 March 2022 *[ST]* is included here by reference.

4 Definitions

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

CA	Certification Authority
CM	Cryptographic Module
CSR	Certificate Signing Request
DTBS	Data to be signed
IT	Information Technology
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OSP	Organizational Security Policies
PP	Protection Profile
PU	Privileged User(s)
QSCD	Qualified Electronic Signature Creation Device or Qualified Electronic Seal Signature Creation Device
QTSP	Qualified Trust Service Provider
RA	Registration Authority
SAD	Signature Activation Data
SAM	Signature Activation Module also referred to as TOE
SAP	Signature Activation Protocol
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Device
SIC	Signer Interaction Component
SPD	Security Problem Definition
SSA	Sign Server Application
SVD	Signature Verification Data
TOE	Target of Evaluation
TRISS	Trust Remote InfoCert Signing Server (TOE) also referred to as (SAM)
TSP	Trust Service Provider
TW4S	Trustworthy Systems Supporting Server Signing

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 “TRISS Trust Remote Infocert Signing Server"– EAL4+, 22-RPT-230, Version 4.0, 01 April 2022

[ETR HW] Evaluation Technical Report “nShield Solo XC Hardware Security Module v12.60.15” – EAL4+, Version 3.0, date: 5 July 2021

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

[PP] Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, 419241-2:2019 v0.16, dated 18 May 2020, registered under the reference ANSSI-CC-PP-2018/02-M01

[ST] Signature Activation Module Trust Remote InfoCert Signing Server – TRISS Security Target, Version 2.1, 31 March 2022

[STAR_DevCenter] Site Audit report Infocert development site, 22-RPT-002, Version 2.0, 28 March 2022

[STAR_DataCenter] Site Audit report Infocert Data Center, 22-RPT-003, Version 2.0, 28 March 2022

(This is the end of this report.)