Certification Report

SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14

Sponsor and developer: ***A.E.T. Europe B.V.***

IJsselburcht 3
6825 BS, Arnhem
The Netherlands

Evaluation facility: ***Riscure B.V.***

Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-2400004-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400004-01**
Author(s):	**Haico Haak**
Date:	**30 September 2024**
Number of pages:	**13**
Number of appendices:	**0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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.

Recognition of the Certificate

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 SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14. The developer of the SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14 is A.E.T. Europe B.V. located in Arnhem, The Netherlands 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 consists of a Java Card applet on top of a Java Card OS and native OS on top of a micro controller. The applet provides PKI and PKCS#15 functionality. The TOE provides the functionality of an eIDAS QSCD with protection of private key material and qualified certificates. In order for applications to communicate with the TOE, the appropriate middleware is required.

The TOE is intended to be used as a portable personal electronic signature creation device in a managed IT environment where the electronic signature is used as proof of authenticity and/or presence of the signatory. The TOE interacts with the environment by means of standard smart card interfaces.

The signatory is required to provide authentication information to the TOE before it creates an electronic signature, thereby preventing unauthorized use of the TOE. The TOE is typically a smart card form factor and could carry printed information about the signatory. This Java Card is a composite.

The TOE may also be used as a qualified seal creation device to create advanced electronic seals. Therefore, any reference to QSCD in this report should be understood to refer to both qualified signature and seal creation devices.

The TOE was previously evaluated by Riscure B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 20 April 2021 (CC-21-0274076). The current evaluation of the TOE has also been conducted by Riscure B.V and was completed on 30-09-2024 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 major changes from previous evaluations are:

- Updates of the underlying platform
- Introduction of a new version containing security and functional updates, of which the major updates concern the addition of new RSA padding support and ECC key management features.
- user guidance and ST updates to reflect the introduction of the new version and associated documentation.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14, 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 SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14 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).

TrustCB 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.

The TOE is stated as a Qualified Signature Creation Device and Qualified Seal Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by Riscure B.V. included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

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.

[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 SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14 from A.E.T. Europe B.V. located in Arnhem, The Netherlands.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware and Software	SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD	v3.0.1.12, or v3.0.1.13 or v3.0.1.14

To ensure secure usage a set of guidance documents is provided, together with the SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14. For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.4.

2.2 Security Policy

The TOE is a composite TOE, consisting of the SafeSign IC PKI applet on (underlying Java Card platform) NXP JCOP 4 P71. The TOE is a Smart Card Integrated Circuit with Embedded Software and SafeSign IC PKI applet, which provides QSCD functionality in accordance to [EU-REG].

The TOE claims compliancy to EN 419 211 Parts 2-3 (Signature Protection Profiles [EN419211-2] and [EN419211-3]).

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 4.2 of the *[ST]*.

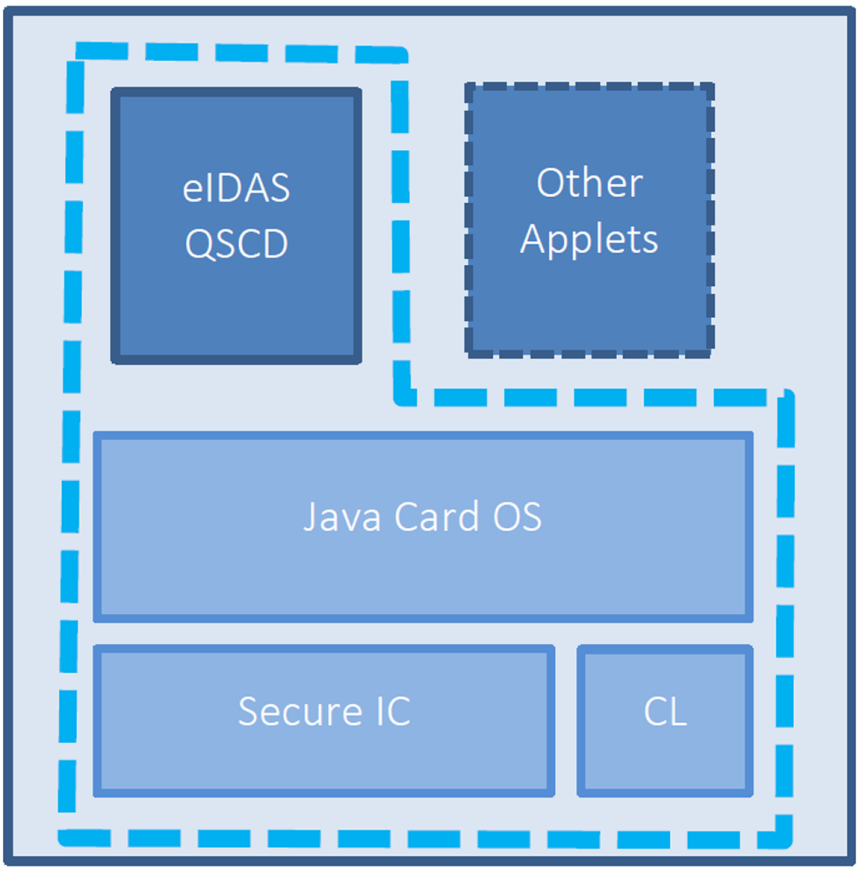
2.3.2 Clarification of scope

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 overview of the composite TOE can be found in the figure below. The dashed line represents the (Composite) TOE boundary. In this boundary are:

- The Secure IC with cryptographic library (CL) combined with the Java Card OS, is the already certified component of the TOE.
- The SafeSign IC PKI applet eIDAS QSCD implementing the TSF.



2.5 Documentation

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

Identifier		Version
SafeSign IC PKI Applet Interface Specification, generated with applet, dependent on applet version	For applet versions 3.0.1.12/3.0.1.13: SafeSign IC PKI Applet v3 Interface Specification	3.4, generated with applet
	For applet version 3.0.1.14: SafeSign IC PKI Applet v3.0.1.14 Interface Specification	2024.0501, generated with applet
Operational Guidance SafeSign IC eIDAS QSCD		v1.13, 2024-09-27
Preparative Procedures SafeSign IC eIDAS QSCD		v1.13, 2024-09-27
Test Report		N/A, generated with applet
Information file		N/A, generated with applet
The public key matching the private key used to sign the application binary file of the applet.		N/A, generated with applet

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 module level. 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 developer provided samples for the testing performed by the evaluators using the Riscure test environment.

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.

2.6.2 Independent penetration testing

The vulnerability analysis is performed based on the structure of the attack methods defined by JHAS [JIL-AMS]. For each attack method, the lab described the objective of the attack and how the attack method applies to the TOE. The following is considered for each attack method:

- Obligations and recommendations for the composite evaluator [HW-ETRfC]
- The design and implementation of the features relevant for the attack method
- Specific attack techniques from the evaluator's attack repository
- Implemented countermeasures
- User guidance

Based on these items, the lab determines whether an attack method is applicable to the TOE and should be tested during the penetration testing phase.

In the baseline evaluation, the total test effort expended by the evaluators was 2 weeks. During that test campaign 100% of the total time was spend on Perturbation attacks.

In this re-certifcation, the total test effort expended by the evaluators was 15 days. During that test campaign, 100% of the total time was spent on Perturbation attacks.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was version 3.0.1.14 and as described in the [ST].

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.

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. The strength of the implementation of the cryptographic functionality has been assessed as part of the evaluation of the underlying JCOP 4 P71 Java Card Platform (see [HW-CERT]).

All key sizes specified for the SafeSign IC PKI applet in the [ST] have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". However, it should be noted that the underlying JCOP 4 P71 platform supports a wider range of key sizes (see [HW-ST]), including those with lesser algorithmic security level than 100 bits as the minimum required for high attack potential (AVA_VAN.5).

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

One site audit was performed as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14. More information on the identification of the TOE and its versions can be found in the [ST], section 1.3.

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 SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13 and 3.0.1.14, 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] and [EN419211-3].

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 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 Applet-TOE does not implement any cryptographic mechanisms; it uses those of the certified underlying platform, as reported in [HW-CERT].

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.

3 Security Target

The SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD Security Target, v1.23, 27 September 2024 *[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:

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
QSCD	Qualified Signature/Seal 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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[eIDAS-REP]	eIDAS conformity assessment for SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD 3.0.1.12, 3.0.1.13, and 3.0.1.14, Document ID 20230148-D15, v1.3, 27 September 2024
[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.
[EN419211-3]	EN 419 211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01.
[ETR]	Evaluation Technical Report for SafeSign IC PKI applet on JCOP4P71eIDAS QSCD3.0.1.12, 3.0.1.13, and 3.0.1.14, Document ID 20230148-D1, v1.3, 27 September 2024
[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]	NSCIB-CC-2300172-01 Certificate JCOP 4 P71, versions: JCOP 4 P71 v4.7 R1.00.4, JCOP 4 P71 v4.7 R1.01.4, JCOP 4 P71 v4.7 R1.02.4, JCOP 4 SE050 v4.7 R2.00.11, JCOP 4 SE050 v4.7 R2.03.11, issued on 04-04-2024
[HW-ETRfC]	Evaluation Technical Report for Composition NXP “JCOP 4 P71” – EAL6+, version 2.0, 13 March 2024
[HW-ST]	JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050, Rev. 4.14, 2024 01-17
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	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 2.6, 02 August 2022
[ST]	SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD Security Target, v1.23, 27 September 2024

(This is the end of this report.)