# Certification Report

# SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD v3.0.1.11

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-224791-CR2**

Report version: **2**

Project number: **224791_2**

Author(s): **Denise Cater**

Date: **06 February 2022**

Number of pages: **11**

Number of appendices: **0**





Headoffice:
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 Dutch Chamber of Commerce 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 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.

# 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.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD v3.0.1.11. The developer of the SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD v3.0.1.11 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 has been originally evaluated by Riscure B.V. located in Delft, The Netherlands and was certified on 24 July 2019. The re-evaluation also took place by Riscure B.V. and was completed on 18 March 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are resulting from re-certification of the underlying platform, coupled with some updates to guidance, the development environment and introduction of an option at the end of the personalisation lifecycle phase.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made, as well as renewed penetration 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 3 P60 eIDAS QSCD v3.0.1.11, 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 3 P60 eIDAS QSCD v3.0.1.11 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 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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

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. It should be noted that the certification results only apply to the specific version of the product as evaluated.

Version 2 of this Certification Report was generated in support of the eIDAS publication of this TOE.

# 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 3 P60 eIDAS QSCD v3.0.1.11 from A.E.T. Europe B.V. located in Arnhem, The Netherlands.

The TOE is comprised of the following main components (which include by reference the platform components listed in *[HW-CERT]*):

| Delivery item type | Identifier | Version |
|---|---|---|
| Hardware & Software | SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD | v3.0.1.11 |

To ensure secure usage a set of guidance documents is provided together with the SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD v3.0.1.11. Details can be found in section 2.5 of this report.

## 2.2 Security Policy

The TOE is a composite TOE, consisting of the SafeSign IC PKI applet on (underlying Java Card platform) NXP JCOP 3 P60. 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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.5 of the *[ST]*.

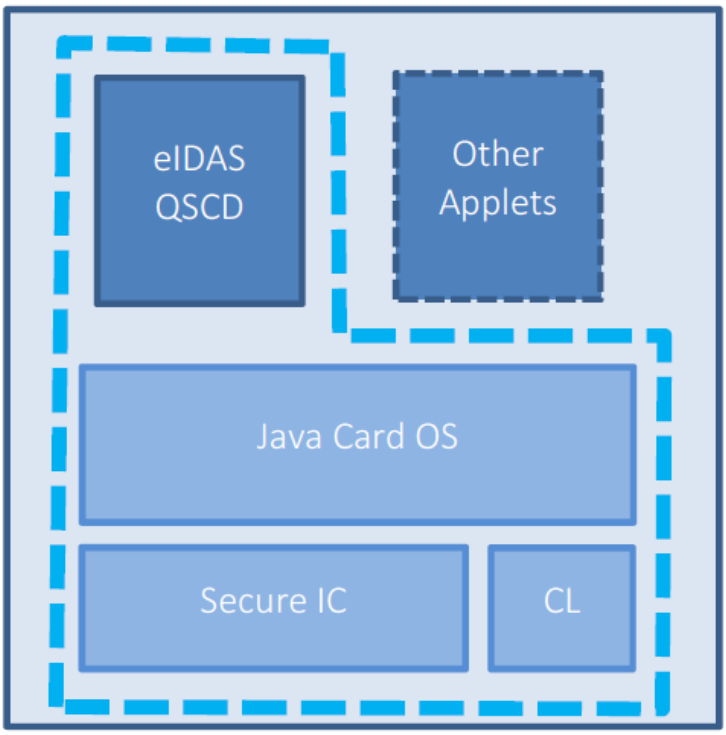
### 2.3.2 Clarification of scope

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 TOE boundary is indicated by the dashed line. 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 |
|---|---|
| Operational Guidance SafeSign IC eIDAS QSCD | v1.1, 08-10-2020 |
| Preparative Procedures SafeSign IC eIDAS QSCD | v1.1, 08-10-2020 |
| SafeSign IC PKI Applet v3 Interface Specification | v3.4, generated with applet |
| Applet 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.

In addition, during the baseline evaluation the evaluators witnessed execution of a selection of the developer tests at the developer site. The developer provided samples for the testing performed by the evaluators using the Riscure test environment.

The underlying platform 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 evaluator independent penetration tests were conducted according to the following vulnerability analysis approach:

- Consideration of Riscure attack repository, which is an internal repository of potential attacks maintained on the basis of the expert knowledge amassed within Riscure.
- Analysis of the TOE design and implementation for resistance against the JIL attacks.
- Analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.
- The evaluators concluded that a small number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently practical penetration testing was performed.

In this re-evaluation the total test effort expended by the evaluators was 10 days. During that test campaign for the re-evaluation 100% of the total time was spend on Perturbation attacks.

### 2.6.3 Test Configuration

Developer and evaluator testing was performed on the TOE as defined in Section 2.1 above, identified using the Get data command “0X00CA010304” the result of which was “0300010B9000”.

Evaluator testing was performed on samples taken from two batches provided by the developer. The differences between the batches (configuration and preparation only) have been analysed and confirmed to have no impact on the test results.

### 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.

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 3 P60 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 3 P60 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 Re-used evaluation results*

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

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were re-used by composition.

One virtual 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 3 P60 eIDAS QSCD v3.0.1.11.

## 2.9 Results of the Evaluation

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 3 P60 eIDAS QSCD v3.0.1.11, 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 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 Applet-TOE does not implement any cryptographic mechanisms; it uses those of the certified underlying platform, as reported in *[HW-CERT].*

# 3 Security Target

The SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD Security Target, v1.4, 22 Feb 2021 *[ST]* is included here by reference.

# 4 Definitions

This list of Acronyms and the glossary of terms 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 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. |
| [ETR] | Evaluation Technical Report for SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD v3.0.1.11, 2020186-D2, Version 1.1, 08 March 2021. |
| [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] | Certification Report NXP JCOP 3 P60, NSCIB-CC-98209-CR4.1, 25 August 2020 (certificate CC-20-98209, date 4th issue 14-01-2020). |
| [HW-ETRfC] | Evaluation Technical Report for Composition NXP JCOP 3 P60 – EAL5+, v.13.0, 13 January 2020. |
| [HW-ST] | JCOP 3 P60 Security Target Lite, Rev 4.0, 2019-08-23. |
| [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. |
| [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. |
| [ST] | SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD Security Target, v1.4, 22 Feb 2021. |


(This is the end of this report).