Certification Report

AKD eID 2.0 SSCD

Sponsor and developer:	***AKD d.o.o.*** **Savska cesta 31,** **10 000 Zagreb,** **Republic of Croatia**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300144-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300144-01**
Author(s):	**Haico Haak**
Date:	**30 September 2024**
Number of pages:	**12**
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 AKD eID 2.0 SSCD. The developer of the AKD eID 2.0 SSCD is AKD d.o.o. located in Zagreb, Republic of Croatia 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 hardware and software configured to securely create, import, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole lifecycle as to be used in a signature creation process solely by its signatory. The TOE is intended as a qualified signature creation device and qualified seal creation device in accordance with Article 29 and Article 39 of Regulation (EU) No. 910/2014.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature:

- to generate or to import signature-creation data (SCD) and the correspondent signature-verification data (SVD),
- to export the SVD for certification through a trusted channel to the CGA,
- to, optionally, receive and store certificate info,
- to switch the SSCD from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation 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 scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the AKD eID 2.0 SSCD, 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 AKD eID 2.0 SSCD 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 ALC_DVS.2 (Sufficiency of security measures) and 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 AKD eID 2.0 SSCD from AKD d.o.o. located in Zagreb, Republic of Croatia.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Smartcard including Personalization key set	AKD eID 2.0 SSCD	2.0 rev8

To ensure secure usage a set of guidance documents is provided, together with the AKD eID 2.0 SSCD. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.

2.2 Security Policy

The TOE is a combination of hardware and software configured to securely create, import, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole lifecycle as to be used in a signature creation process solely by its signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature:

- to generate or to import signature-creation data (SCD) and the correspondent signature verification data (SVD),
- to export the SVD for certification through a trusted channel to the CGA,
- to, optionally, receive and store certificate info,
- to switch the SSCD from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data.

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 TOE is a combination of hardware and software, embedded in a smartcard form. The TOE provides user authentication and cryptographic services to securely create, import, use and manage signature creation data (SCD). The Application-TOE (developed by AKD) is installed on top of an NXP JCOP 4.5 P71 platform. The AKD eID 2.0 SSCD can be installed alongside additional applets. The TOE applet disallows other applets to be installed after it has been configured, preventing additional applets to be installed post-issuance. The diagram below shows the components of the TOE. The

Application-TOE boundary is marked red.

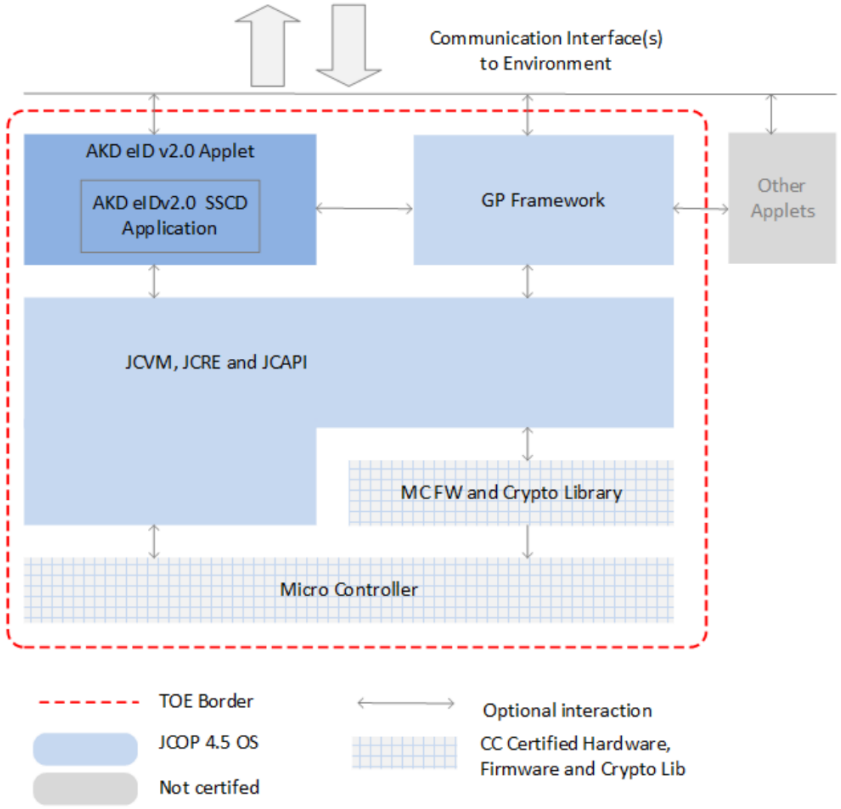

Figure 1: Composite TOE components

The TOE is named "AKD eID 2.0 SSCD". It is available in a single configuration.

2.5 Documentation

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

Identifier	Version
AKD Electronic Identity Card User Guidance.	v1.12

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 extensively used to verify that the functions return the expected values.

The test results of the underlying base TOE are extendable to composite evaluations, as the base TOE is used 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 verified the execution of a selection of the developer tests, and conducted a number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The VA focused on the functionality implemented by the applet TOE, but considers the entire composite TOE where needed. Any potential vulnerabilities that may arise from the usage of the underlying platform are considered and assessed. The assessment is structured based on the JHAS attack methods for smartcards and similar devices [JIL.AMS].

For each attack method, it is described how the attack method applies to the TOE. The following is considered foreach attack method:

- The design and implementation of the features relevant for the attack method
- Specific attack techniques from the evaluator's attack repository
- Implemented countermeasures
- Observations from the platform evaluation
- Platform user guidance

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

During the assessment, the evaluator also examined the results of the evaluation of the underlying platform, and confirmed that any obligations or guidance from the platform have been correctly covered and followed.

In total two Fault Injection attacks and one Logical attack was performed as part of the independent penetration testing effort.

The total test effort expended by the evaluators was 8 weeks. During that test campaign, ; 62.5% of the total time was spent on TOE characterization, 25% on Perturbation attacks, 0% on side-channel testing, and 12.5% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*. The state of the TOE that is tested is the OPERATE state.

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.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number AKD eID 2.0 SSCD.

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 AKD eID 2.0 SSCD, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5 and ALC_DVS.2**. 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], [EN419211-3], [EN419211-4], [EN419211-5], [EN419211-6]

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: None.

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 Security Target AKD eID 2.0 SSCD, v2.4, 20 September 2024 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PKI	Public Key Infrastructure
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
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
[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 AKD eID 2.0 SSCD, 20230029-D15, Version 1.1, 20 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.
[EN419211-4]	EN 419211-4:2013 Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, Version 1.0.1, 2013-11-27, 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, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01.
[EN419211-6]	EN 419211-6:2014 Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application, Version 1.0.4, Registered under the reference BSI-CC-PP-0076- 2013-MA-01.
[ETR]	Evaluation Technical Report for AKD eID SSCD 2.0, 20230029-D1, Version 1.2, 20 September 2024
[PLT-CERT]	JCOP 4.5 P71 certificate NSCIB-CC-2300127-01, issued 16-01-2024
[PLT-ETRfC]	Evaluation Technical Report for Composition “NXP JCOP 4.5 P71” – EAL6+, 23-RPT-1350, version 2.0, 20 December 2023
[PLT-ST]	JCOP 4.5 P71 Security Target Lite for JCOP 4.5 P71, Revision 2.6, 11 December 2023
[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]	Security Target AKD eID 2.0 SSCD, v2.4, 20 September 2024
[ST-lite]	Security Target Lite AKD eID 2.0 SSCD, v2.4, 20 September 2024

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)