Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1130-2021

for

fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5

from

fiskaly GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1130-2021 (*)

Fiscalization

fiskaly Security Module Application for Electronic Record-keeping Systems
Version 1.0.5

from	fiskaly GmbH
PP Conformance:	Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 July 2020, BSI-CC-PP-0105-V2-2020
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_LCD.1 and ALC_CMS.3

SOGIS
Recognition Agreement for components up to EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement recognition for components up to EAL 2

Bonn, 17 May 2021

For the Federal Office for Information Security

DAkkS
Deutsche Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola L.S.
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5 has undergone the certification procedure at BSI.

The evaluation of the product fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 20 April 2021. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: fiskaly GmbH.

The product was developed by: fiskaly GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 17 May 2021 is valid until 16 May 2029. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed,
4. to conduct a reassessment after 5 years in order to assess the robustness of the product against new state-of-the-art attack methods. This has to be done on the developer‘s own initiative and at his own expense. As evidence a report regarding a reassessment or a re certification according to the regulations of the BSI certification scheme shall be provided.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] fiskaly GmbH
Stutterheimstraße 16-18/2/20e
1150 Wien
Österreich

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5 provided by fiskaly GmbH.

It is a Security Module application for Electronic Record-keeping Systems implemented as software. The TOE is a local software library that will run within a TSE that implements the client-server architecture running on a platform supporting secure storage of assets.

The TOE relies on the fiskaly Cloud Crypto Service Provider (BSI-DSZ-CC-1153-2021) as a Cryptographic Service Provider Light (CSPL) for all cryptographic operations except for the TOE sided implementation of the Trusted Channel which is implemented using the Password Authenticated Connection Establishment (PACE) protocol [9] by the TOE itself. This CSPL is not part of this TOE.

The TOE provides the following functions:

- Generation of Log messages
- Security Management functions
- Audit records
- Import of Transaction Data from and Export of Log message to CTSS interface component
- Identification of external entities (CSPL,CTSS) and authentication of Administrators
- Test of external entities (CSPL, CTSS)
- Self-test and secure state
- Secure download and authorized use of Update Code Package
- Secure Import and Export of User Data
- Secure communication between TOE and CSPL via Trusted Channel

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 July 2020, BSI-CC-PP-0105-V2-2020 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2 augmented by ALC_LCD.1 and ALC_CMS.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF_SecMan	Security Management
SF_IdAuth	User Identification and Authentication
SF_UserDataProt	User Data Protection

TOE Security Functionality	Addressed issue
SF_TSFProt	Protection of the TSF
SF_Audit	Security Audit
SF_UcpImp	Code Update Package Import
SF_TrustChan	Trusted channel between TOE and CSPLight

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	The delivered item is a docker image containing the TOE.	Docker image reference/name as provided by fiskaly GmbH: IMAGE="$REGISTRY/fiskaly/smaers: 1.0.5"	The docker image containing the TOE will be delivered via TLS-protected download to the integrator who checks the TOE version number using the command ‘GetStatus’ and the TOE’s authenticity and integrity as described below. He installs and personalizes the TOE which is then delivered to the taxpayer.

No	Type	Identifier	Release	Form of Delivery
2	DOC	Preparative Procedures & Operational User Guidance Documentation fiskaly Security Module Application for Electronic Record-keeping Systems Version 1.0.5 [11]	Version: 1.1.6 Date: 2021-05-11 SHA256: C1619B31A188C7CB91DCA21BFC13CBEBAF269FF4F01AD65DB3BF8E6BB13B2357	Signed Documents via Google Cloud storage download and E-Mail.
3	DOC	Functional Specification Documentation fiskaly Security Module Application for Electronic Record-keeping Systems Version 1.0.5 [12]	Version: 1.1.4 Date: 2021-05-06 SHA256: 423198F8B631EB9F48F2C2397891917B59810BF63FD43DB231588227FEC4254C	Signed Documents via Google Cloud storage download and E-Mail.
4	SW	Digital signature file	smaers-linux-amd64.minisig	Same as first entry of this table.

Table 2: Deliverables of the TOE

Please not that for its operation, the TOE needs the following hardware and software requirements fulfilled in its environment.

- Cryptographic Service Provider Light (CSPLight or CSPL) with CC EAL2 certification. The CSPL used in the TOE is fiscaly Cloud Crypto Service Provider, Version 1.2.0, BSI-DSZ-CC-1153-V2.
- General purpose hardware, e.g. PC, laptop or server hardware.
- Operating System Alpine Linux Version 3.x, where the TOE is run in Docker 19.
- Mass storage device for persisting signed transaction logs.
- Secure mass storage device for persisting internally stored data.

Delivery of sensitive electronic data and guidance documentation is protected by an electronic signature and performed by using Google Cloud storage download and via E-Mail. The guidance documentation is delivered to the integrator who forwards necessary information to the taxpayer according to chapter 6 of [11], including the public key fingerprint of the root CA and the method how to verify it.

The Security Module Application for Electronic Record-keeping Systems is provided as software. The integrator shall check its authenticity as follows:

```
# run minisign within an emphemeral docker container:
2 docker run --rm $IMAGE minisign \
3 -P RWRUupxsFLBrtFlb7g2ZWVFSQE23BvMEtPszqNu2E8Q32U4L99AKexpl \
4 -Vm smaers-linux-amd64
```

The *minisign* tool The minisign tool is an Alpine Linux package and part of the used Linux distribution. It requires the detached digital signature file (i.e. *smaers-linux-amd64.minisig*) that is provided by fiskaly GmbH as well.

To ensure that the provided public key is genuine it shall be compared with the public key contained and published in the Security Target [6] and here:

RWRUupxsFLBrtFlb7g2ZWVFSQE23BvMEtPszqNu2E8Q32U4L99AKexpl.

No individual public key for each TOE instance will be generated.

To check the version of the TOE, the integrator and the taxpayer need to export a TAR-file from the TOE and consider the file *info.csv* within. The field *version* in this file contains the version of the TOE and of the CSPL, for example the entry `fiskaly sign cloud-TSE v1.0.5-1.2.0` refers to SMAERS version 1.0.5 and CSPL version 1.2.0.

The TOE is the Security Module Application for Electronic Record-keeping Systems, TOE Version: 1.0.5.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE implements a role-based access control policy to control administrative access to the system. In addition, the TOE implements policies pertaining to the following security functional classes:

- Security Management,
- User Identification and Authentication,
- User Data Protection,
- Protection of the TSF,
- Security Audit,
- Code Update Package Import,
- Trusted Channel between TOE and CSP Light.

Specific details concerning the above mentioned security policies can be found in chapter 6.1 of the Security Target [6].

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The topics listed in chapter 4.2 of the ST [6] are of relevance.

5. Architectural Information

The TOE is a software TOE running on dedicated non-TOE hardware (server) as well as dedicated non-TOE software (The Operating System is Alpine Linux Version 3.x, where the TOE is run in Docker 19), building the non-TOE platform. The non-TOE platform is expected to provide protection against physical intrusion and tampering, the protection mechanisms by the environment and non-TOE hardware platform are described in the document “Umgebungsschutzkonzept” [13].

The SFR-enforcing subsystems of the TOE are *interfaces/CSPL, TrustedChannel, interfaces/ERS, SMAERS, TR*

The subsystem *"interfaces/CSPL"* forwards data between subsystem SMAERS and subsystem Trusted Channel and parses and encodes data on the way.

The subsystem *"TrustedChannel"* implements PACE which uses Curve P-256 as specified in FIPS 186-4. To realize the trusted channel, the subsystem uses the AES implementation of the *go* standard library.

The subsystem *"interfaces/ERS"* receives *Protobuf* Requests from ERS. It parses the incoming *Protobuf* messages and dispatches them to subsystem TR. To do so, subsystem TR registers one handle for each request and subsystem interfaces/ERS decides which handle needs to be invoked based on the parsed message. After subsystem TR finishes the execution, subsystem interfaces/ERS encodes the response as *Protobuf* response and transmits the serialized result back to the invoking ERS via the HTTP connection.

The subsystem *"SMAERS"* provides the following security functionality: Management of the the key assets of the TOE; Tracking of TOE operations; Reception of transaction data and forming and management of log messages; Ensuring that only one function is executed at any time; Implementation of the DRNG of the TOE; Storage of log messages to be singled later; User management and access control; Enforcing of periodic selftests every 24h.

The subsystem *"TR"* provides the following security functionality: Ensuring that only one function is executed at any time; Data Export and Deletion; User management and access control.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The TOE test configuration is defined by the notation "fiskaly Security Module Application for Electronic Record-keeping Systems Version 1.0.5."

The exact version number of the TOE verified.

The TOE is running and was tested in Docker 19 on the underlying operating system Alpine Linux 3.12.0

Developer Tests

The tests are performed on a test system running a virtual machine, containing the Docker container running the TOE. The tested TOE version is 1.0.5.

The virtual machine *“SMAERS-TEST-VM”* ran on an Ubuntu Linux 20.04 LTS Server located on a virtualization server.

In addition to the Operating System, the following tools were installed:

- Docker Engine (for running the TOE)
- Go (for running unit tests)

- Task (for running unit tests)
- Java/OpenJDK (for running TSFI tests, manual tests and *mitmproxy*)
- Git (for accessing the source code repository)

The developer tested all TOE Security Functions. TSFI tests were related to all functions which are represented the external interfaces of the TOE. Internal functionality that is not directly accessible from the outside, was tested via unit tests. This was specifically the case for all cryptographic primitives used by the TOE. For all commands and functionality tests, test cases are specified in order to demonstrate the expected behaviour. The developer tests cover all interfaces. The developer testing includes 365 test functions covering all TSFIs and operations, which results in 514 automated tests.

All test cases were executed successfully and ended up with the expected results.

Repetition of Developer Tests by the Evaluator

Repetition of developer tests were performed by the evaluators during the independent evaluator tests. The evaluators have tested the TOE systematically against basic attack potential during their penetration testing.

All achieved test results correspond to the expected test results.

The tests are performed on a test system running a virtual machine, containing the Docker container running the TOE. The tested TOE version is 1.0.5.

The tests performed can be categorized into two groups: unit and TSFI tests.

The test environment is configured by the developer and does not need any actions by the evaluator to run the tests. This means that all necessary configuration files and flags are set.

Independent Evaluator Tests

Tests were performed on a virtual machine installed on a physical server of the developer, as well as the cloud and hardware of the evaluator.

The evaluators verified that the tested version 1.0.5 of the TOE was compliant with the provided documentation.

The evaluators repeated all developer tests, including TSFI, unit and manual tests. The developer tests already cover all TSFIs. Since the evaluators repeated the complete list of developer tests, all given interfaces were covered by the testing. Additionally the following independent evaluator tests were performed:

- Fuzzing of the HTTP-Endpoint.
- The TOE correctly handles out of bounds exceptions.
- The TOE correctly handles out of bounds exceptions.
- Statistical tests of provided hardware based random numbers via the AIS31 statistical test suite.
- Check that the TOE requires a CSP-Light to run.
- Check the correct implementation of the trusted channel between TOE and CSP-Light.
- The TOE correctly checks user roles.

The evaluators determined that all tests were executed successfully and with the expected results.

Penetration tests

The configuration respectively the version of the TOE can be retrieved by the command *GetStatus*. The evaluators verified that the tested version 1.0.5 of the TOE was compliant with the provided documentation.

The evaluators performed a theoretical vulnerability analysis followed by penetration tests for possible attack scenarios.

The tests were performed remotely on a virtual machine running in a test environment of the developer. The environment included the TOE virtual machine and all necessary resources to conduct those tests.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Basic was actually successful in the TOE's operational environment as defined in the Security Target [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following TOE version: fiskaly Security Module Application for Electronic Record-keeping Systems, Version 1.0.5. It is defined by the items in table 2 of this report and by descriptions in the security target [6]. The components of the TOE are defined by the TOE configuration list [10].

It is a security module application implemented as software. It is running on a device that is communicating with the CSP via a trusted channel (referred to as client-server architecture).

The transformation of the TOE into a product consists of several phases that happen without the involvement of the taxpayer. The taxpayer will finally use the TOE within a product. The Hardware Installation, TOE Installation and Personalization comprise the integration of the TOE into its operational Environment. Integrating the Software Interface of the TOE into the ERS Software does not touch the TOE and its life cycle. It is done by ERS-Manufacturer before the ERS can use the TOE. This integration does not require steps on the TOE side. Please note that the ERS-Manufacturer integrates the TOE Interface into the ERS-System while the SMAERS Administrator performs the setup of the TOE in its operational environment. The guidance [11] mainly addresses those roles. If necessary, the ERS-Manufacturer will have to forward certain required resulting information to the End-User / Tax Payer / ERS-User. [11] addresses the mandatory installation, preparative procedures and start-up process of the TOE.

Platform information as well as the setup of the operational environment is described in the USK [13]. This document is relevant for the SMAERS Administrator and not part of the officially evaluated guidance but has been used to set up the correct test environment for the evaluation.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_LCD.1 and ALC_CMS.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 July 2020, BSI-CC-PP-0105-V2-2020 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by ALC_LCD.1 and ALC_CMS.3

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Authentica-tion/ Authenticity	ECDSA Digital Signature generation with SHA	[FIPS 186-4]	P-256	FMT_MSA.4
2	Key Agreement (for PACE)	EC-DH	[FIPS 186-4]	P-256	FCS_CKM.1
3	Integrity	CMAC with AES	[NIST-SP800-38B]	256	FCS_COP.1
4	Trusted Channel	PACE	[TR-03110-2] (PACE)	see above for ‘Key Agree-ment’	FCS_CKM.1
5	Crypto-graphic Primitive	RNG	DRG.3 according to [AIS20], NTG.1 according to [AIS20]	≥ 125 bits of entropy	FCS_RNG.1 Seed length 512 bits entropy + 64

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
					bits nonce + 256 bits personalization

Table 3: TOE cryptographic functionality

Reference details for table 3:

***[FIPS 186-4]**:* *Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).*

***[NIST-SP800-38B]**:* *NIST SP800-38B, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST).*

***[TR-03110-2]**:* *BSI - Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016-12-21, Bundesamt f ür Sicherheit in der Informationstechnik.*

***[AIS20]**:* *Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, AIS20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik*

For all applicable entries of cryptographic algorithms listed in the table above, the Security Level provided is greater than 100 bit.

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs 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 of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The environmental protection concept [13] is a procedural guide with steps for setting up the environmental platform for the TOE. It addresses the SMAERS administrator in the context of the assumption A.Admin and the Security Objectives for the Operational Environment OE.SecOEnv as well as OE.SMAERSPlatform and OE.SecUCP. The

SMAERS administrator is therefore responsible to ensure that the platform is set up securely according to the concept described in [13].

The CTSS shall be installed according to [13]. For this [13] shall be delivered to the user installing the CTSS as required in [11] together with the CTSS that integrates the TOE.

Instructions for the integrator about which information has to be forwarded to the tax payer can be found in chapter 6 of [11].

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CA	Certification Authority
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CSP	Cryptographic Service Provider
CSPL	Cryptographic Service Provider Light
CTSS	Certified Technical Security System
EAL	Evaluation Assurance Level
ERS	Electronic Record-keeping Systems
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PACE	Password Authenticated Connection Establishment
PP	Protection Profile

SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMAERS	Security Module Application for Electronic-keeping Systems
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1130-2021, Security Target fiskaly Security Module Application for Electronic Record-keeping Systems TOE Version 1.0.5, Version: 1.1.6, Date: 2021-05-11, fiskaly GmbH

[7] Evaluation Technical Report BSI-DSZ-CC-1130-2021, fiskaly Security Module Application for Electronic Record-keeping Systems Version 1.0.5, Version 1.96, Date: 12.05.2021, SRC Security Research & Consulting GmbH, (confidential document)

[8] Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 July 2020, BSI-CC-PP-0105-V2-2020

[9] BSI - Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016-12-21, Bundesamt für Sicherheit in der Informationstechnik

[10] Configuration list for the TOE, cl.csv as provided by the developer on 2021-05-11 with accompanying SHA256 value 119C677A27C8EBAA14C8E240C5CC29AE8E-08FF19468C959883569A74FAF5A9CB, fiskaly GmbH (confidential document)

[11] Preparative Procedures & Operational User Guidance Documentation fiskaly Security Module Application for Electronic Record-keeping Systems TOE Ver-sion 1.0.5, Version: 1.1.6, Date: 2021-05-11, fiskaly GmbH (confidential document)

[12] Functional Specification Documentation fiskaly Security Module Application for Electronic Record-keeping Systems TOE Version 1.0.5, Version: 1.1.4, Date: 2021-05-06 , fiskaly GmbH (confidential document)

[13] Umgebungsschutzkonzept fiskaly Security Module Application for Electronic Record-keeping Systems TOE Version 1.0.5, Version: 1.3.5, Date: 2021-04-21, fiskaly GmbH (confidential document)

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report