Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1153-V5-2025

for

fiskaly Cloud Crypto Service Provider, Version 1.5.0

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-1153-V5-2025 (*)

Cryptographic Service Provider Light

fiskaly Cloud Crypto Service Provider
Version 1.5.0

from	fiskaly GmbH
PP Conformance:	Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Version 1.0, 26 February 2020, BSI-CC-PP-0113-2020
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_CMS.3, ALC_LCD.1
valid until:	2 July 2030

SOGIS
Recognition Agreement

Common Criteria

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022. 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.

Bonn, 3 July 2025

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Director-General

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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 licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022[4] [1] also published as ISO/IEC 15408

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 Methodology for IT Security Evaluation (CEM), CC:2022 [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.

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

[4] Proclamation of the Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

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 Cloud Crypto Service Provider, Version 1.5.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1153-V3-2021. Specific results from the evaluation process BSI-DSZ-CC-1153-V3-2021 were re-used.

The evaluation of the product fiskaly Cloud Crypto Service Provider, Version 1.5.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 23 June 2025. 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 evaluated guidance documentation and in the following report, are observed,
- the product is operated in the environment 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. 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. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

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 3 July 2025 is valid until 2 July 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

[5] Information Technology Security Evaluation Facility

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.

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 Cloud Crypto Service Provider, Version 1.5.0 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)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
Mariahilfer Straße 36/5, 4. OG
AT-1070 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 Cloud Crypto Service Provider, Version 1.5.0. It is intended to be used with products requiring a certified Cryptographic Service Provider Light (CSPLight).

The Security Target [5] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Version 1.0, 26 February 2020, BSI-CC-PP-0113-2020 [7].

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_CMS.3, ALC_LCD.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. 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
Key management functionality	The key management functionality covers the security functionality related to key management and administration which only allows management of cryptographic keys and other management functions to authorized roles. It includes functionality for key generation, key derivation and key agreement, internal storage of keys, import and export of keys with protection of their confidentiality and integrity.
Data encryption	The TOE provides the symmetric data encryption and decryption algorithm AES with standardized key lengths of 128 and 256 bits.
Hybrid encryption with message authentication code	The TOE provides hybrid data encryption/decryption and MAC calculation/verification of user data.
Data integrity mechanisms	The TOE provides data integrity protection by symmetric and asymmetric cryptography.
Authentication, attestation, trusted channel	The TOE provides a cryptographically protected trusted communication channel between the TOE and external entities as well as the authentication of external entities.
User identification and authentication	The TOE implements user identification and authentication, all subsystems implementing TSFI must perform this before giving access to the specific TOE services.
Access control	The TOE enforces a strict role based access control. The roles associated with the authenticated user and user’s current status define the authorization and allowed use of services and objects.
Security management	The TOE provides administrative services such as management of security functions, roles and attributes.
TOE security functionality protection	The TOE performs tests of the TOE integrity, TSF data integrity, access control system and cryptographic functionality.

TOE Security Functionality	Addressed issue
Update Code Package	The TOE supports downloading, integrity and authenticity verification and decryption of Update Code Packages (UCP). The functionality requires to be authenticated by a user with the Update Agent role.
Time stamping	The TOE provides a time stamp service. All time-related services take place using access to the TOE's internal system clock which is synchronized using a trusted time service via an authenticated Network Time Security (NTS) service provider.
Clustering of TOEs for scalability of performance and availability	The TOE supports clustering of a single master node and multiple slave nodes to improve the availability of the TOE.
Generation of audit records	The TOE generates audit records on selected user activities and security events of the TOE. Audit records are exported by the TOE in signed and time stamped form.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5], 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 [5], chapters 3.4, 3.2 and 3.3.

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 Cloud Crypto Service Provider, Version 1.5.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	fiskaly Cloud Crypto Service Provider	TOE Version: 1.5.0	Physical delivery of the signed JAR file to the customer via a fiskaly GmbH representative
2	DOC	Preparative Procedures & Operational User Guidance Documentation	Document Version: 1.5.1, Date: 20.01.2025	Download via a web portal or send by e-mail
	SHA256: d1c55a8c897f8b315623ab33ca0d69daea49829a80978845b69072877bb7dcf9			

Table 2: Deliverables of the TOE

The fiskaly Cloud Crypto Service Provider is provided as a pure software. Even though the fiskaly Cloud Crypto Service Provider is personally delivered, the customer shall check its authenticity as follows:

```
1 $ minisign -P
RWRUupxsFLBrFlb7g2ZWVFSQE23BvMEtPszqNu2E8Q32U4L99AKexpl -V -m
cspl.jar

2 Signature and comment signature verified

3 Trusted comment : timestamp :1603971010 file : cspl.jar
```

The minisign tool requires the detached digital signature file (i.e. cspl.jar.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 (cf. [5]): RWRUupxsFLBrtFlb7g2ZWVFSQE23BvMEtPszqNu2E8Q32U4L99AKexpl.

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

As the TOE is a JAR file, it is also digitally signed using an EV code signing certificate. This signature shall be checked by using the following command

```
1 $ jarsigner - verify cspl.jar

2 jar verified
```

The TOE version can be checked after the installation and setup of the TOE via the HTTP endpoint/api/v1/rc/app by sending the message

```
Version.Request
```

The TOE is fiskaly Cloud Crypto Service Provider, TOE Version: 1.5.0 according to [5].

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Key management
- Data encryption
- Hybrid encryption with MAC for user data
- Data integrity mechanisms
- Time Stamp
- Authentication and attestation of the TOE, trusted channel
- User identification and authentication
- Access control
- Security Management
- Security Audit
- Protection of the TSF
- Import and verification of Update Code Package
- Clustering

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 following topics are of relevance:

- OE.CommInf: Communication infrastructure,
- OE.AppComp: Support of the Application component,
- OE.SecManag: Security management,
- OE.SecComm: Protection of communication channel,
- OE.SUCP: Signed Update Code Packages,
- OE.SecPlatform: Secure Hardware Platform,
- OE.Audit: Review and availability of audit records,
- OE.TimeSource: External time source,
- OE.ClusterCtrl: Control of the cluster, and
- OE.TSFdataTrans: Transfer of TSF data within the CSPLight cluster.

Details can be found in the Security Target [5], chapter 4.2.

5. Architectural Information

The TOE is a software TOE running on dedicated non-TOE hardware (PrimeKey SEE server or Private Machines Enforcer Server) as well as dedicated non-TOE software (Alpine Linux, JVM), building the non-TOE platform. The TOE is operated on a hardware platform, either PrimeKey SEE (FIPS 140-2 Level 3 certification expired on 10.03.2024) or Enforcer R2 (ongoing FIPS 140-3 Level 4 certification process). The non-TOE hardware platform is expected to provide protection against physical intrusion and tampering. Additionally, the TOE protects itself from tampering by untrusted entities due to its SFR-enforcing subsystems. The non-TOE software is an Alpine Linux distribution with a minimal functionality. The JVM is configured to allow only JAR files signed by the fiskaly GmbH to access the net and any data on the disk.

The SFR-enforcing subsystems of the TOE are:

- Server subsystem
- Cryptographic subsystem

The server subsystem provides the following security functionality:

- Regular time synchronization
  The server runs a timer that triggers the synchronization of date and time every 24 hours
- Access control
  The server system will check for each implemented function if the calling user has the role that is required for the operation. If this is not the case, an error will be returned and the function will be terminated.
- Auditing functionality
  The server system will provide the audit log messages for the function implementations.

- Key management
  The server system has functions implemented for key related functionality, e.g. such as derivation, deleting, export generation of keys.
- Role management
  The server system provides functionality for managing the timeout values for roles.
- Attestation
  The server system can verify the identity and functionality of the TOE.
- Cluster management
  The server system has functions implemented for cluster related tasks, e.g. such as data export, master and slave assignment and deletion and cluster status retrieval.
- Encryption / Decryption
  The server system provides the functionality to encrypt and decrypt data via an ECKA-EG or RSA-AES scheme.
- Random number generation
  The server system provides the functionality to return random bytes to the requesting caller.
- Signature
  The server system provides the functionality to generate and verify signatures.
- Authentication
  The server system implements functions to manage the authentication of users, e.g. such as resetting and updating entity passwords.
- PACE
  The server system identifies a client to the TOE and sets up the parameters of PACE that shall be used in further communication, thus establishing a secure communication channel with the client.
- UCP
  The server system provides the functionality to update the TOE.

The cryptographic subsystem uses amongst others the following functionality of Bouncy Castle:

- Hash generation using SHA-2
- RSA based signature creation and verification
- RSA key generation
- EC key generation
- ECDSA generation and verification
- Parsing of X.509 certificate
- Random Number Generation

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

7.1. Summary

The developer tested all TOE Security Functions. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour. Repetition of developer tests were performed during the independent evaluator tests.

The evaluators have tested the TOE systematically against basic attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

7.2. Developer Testing

TOE test configuration

The tests are performed on a test system running two virtual machines, the TOE-VM and the Test-VM. The tested TOE version is 1.5.0.

Testing approach

The developer tests cover all interfaces and the random number generator of the two supported underlying hardware platforms.

The tests performed can be categorized into three groups: unit, TSFI and manual tests. Additionally the entropy of random numbers can be tested using the SP-800-90B entropy assessment tool.

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.

Amount of developer testing performed

The developer testing includes, for each supported hardware platform, 465 test functions covering all TSFIs and operations, which results in 3114 automated tests and 6 manual tests.

Testing Results

All test cases were executed successfully and ended up with the expected result. If necessary the developer gives additional annotations.

7.3. Independent Testing

Test Configuration

The TOE test configuration is defined by the notation: fiskaly Cloud Crypto Service Provider Version 1.5.0 (as stated in [5]).

The configuration respectively the version of the TOE can be retrieved from the test environment via the test function cc.tsfi.basic.VersionTest.TestAuthorized(). The evaluators verified that the tested version, 1.5.0, of the TOE is compliant with the provided documentation.

Subset size chosen

The evaluators repeated all developer tests on the Enforcer platform, and all developer tests excluding the cluster tests on the PrimeKey platform.

Selection criteria for the interfaces and interfaces tested

The developer tests cover all TSFIs. Since the evaluators repeated the complete list of developer tests, all given interfaces are covered by the testing.

Additional evaluator tests

Additional the following independent evaluator tests were performed:

- T_User: User roles are changed and relevant tests repeated.
- T_Auditor: Complying FIA_UAU.1.1(3).
- T_Fuzzing: Fuzzing of the HTTP-Endpoint.
- T_Log: Testing in the case of full storage.
- T_Random: Entropy test of generated random numbers

The evaluators determined that all tests were executed successfully. For the penetration tests see below.

7.4. Penetration Testing

Overview

The penetration testing was carried out in the test environment provided by the developer.

All configurations of the TOE being intended to be covered by the current re-evaluation were tested, i.e. version 1.5.0 on both supported hardware platforms.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic was actually successful.

Penetration testing approach

The approach is to try to inject arbitrary data into the TOE by a fuzzing attack on the Secure RPC interface. Since the TOE accepts only communication via the combined protobuf and PACE protocol, this means to overcome the protection of the protocol used for data import.

TOE test configurations

The tested configuration of the TOE is 1.5.0. The testing was carried out on the non-TOE hardware. A script was used in order to try to inject arbitrary data into the TOE endpoint.

Attack scenarios having been tested

The attack scenario that has been tested is “Fuzzing attack on the Secure RPC endpoint in order to inject malicious code”.

SFRs penetration tested

The following SFRs were covered by the penetration tests:

FDP_ITC.2/UD

The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE’s operational environment also including an attacker with a Basic attack potential.

Verdict for the sub-activity

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 [5] provided that all measures required by the developer are applied.

8. Evaluated Configuration

The TOE test configuration is defined by the notation:

- fiskaly Cloud Crypto Service Provider, Version 1.5.0
- The guidance documentation Preparative Procedures & Operational User Guidance Documentation, Document Version 1.5.1

The exact version number of the TOE has been gathered by using the version.request command test case and is for the TOE the version number 1.5.0.

The TOE is running on either the hardware platform PrimeKey SEE or Private Machines Enforcer R2 with OpenJDK 17 on alpine GNU/Linux based on BusyBox.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] 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.

For RNG assessment the scheme interpretations AIS 20 and 31 were used (see [4]).

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_CMS.3, ALC_LCD.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1153-V3-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was the switch from NTP to NTS for synchronising the system time, the addition of new interfaces, bug fixes, updates to dependencies, and the new hardware platform.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Version 1.0, 26 February 2020, BSI-CC-PP-0113-2020 [7]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by ALC_CMS.3, ALC_LCD.1

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 120 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. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
1	Hashing	SHA-256, SHA-384, SHA-512	[FIPS180-4]	none	yes
2	Random Number Generation	RNG	[SP800-90A]; DRG.3	≥ 125 bits of entropy	yes
3	Key Generation	AES	[ISO18033-3]	128, 256	yes
4	Key Derivation	AES	[SP800-56C]	128, 256	yes
5	Key Generation	Curve P-256	[FIPS186-4] B.4 and D.1.2.3	256	yes
6	Key Derivation	Curve P-256 with X9.63	[FIPS186-4] B.4 and	256	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
		Key Derivation Function	D.1.2.3, [TR-03111], chapter 4.3.3		
7	Key Generation	RSA	[RFC8017]	4096	yes
8	Key Agreement	ECDHE Curve P-256 and 256-bit random ECP group	[TR-03111]	128, 256	yes
9	Key Derivation	ECKA-EG Curve P-256 with X9.63 Key Derivation Function	[TR-03111], chapter 4.3.2.2	128, 256	yes
10	Key Generation	ECKA-EG Curve P-256	[FIPS186-4] B.4 and D.1.2.3	256	yes
11	Key Generation	AES-RSA Key generation and RSA encryption	[ISO18033-3], [RFC8017]	128, 256	yes
12	Key Derivation	AES-RSA key derivation and decryption	[ISO14888-2]	128, 256	yes
13	Key Wrapping	AES Key Wrap with padding	[SP800-38F]	128, 256	yes
14	Confidentiality Protection	AES in CBC mode	[SP800-38A], [ISO18033-3], [ISO10116]	128, 256	yes
15	Confidentiality with MAC	AES in CBC mode with CMAC	[SP800-38A], [SP800-38B]	128, 256	yes
16	MAC	AES with CMAC	[SP800-38B]	128, 256	yes
17	Digital Signatures	ECDSA Curve P-256	[FIPS186-4] B.4 and D.1.2.3	256	yes
18	Digital Signatures	RSA and EMSA-PSS	[ISO14888-2], [RFC8017]	4096	yes
19	Trusted Channel	Chip Authentication Version 2	[TR-03110-2], section 3.4	128, 256	yes
20	Trusted Channel	Terminal Authentication Version 2	[TR-03110-2], section 3.3	128, 256	yes
21	Trusted Channel	PACE Curve P-256	[ICAO-9303-11], section 4.4	128, 256	yes
22	Trusted Channel	AES in CBC mode	[SP800-38A], [FIPS197]	128, 256	yes
23	Trusted Channel	AES CMAC	[SP800-38B], [FIPS197]	128, 256	yes
24	Verification of digital signature	ECDSA Curve P-256	[TR-03111]	256	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
	of the Issuer				

Table 3: TOE cryptographic functionality

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.

11. Security Target

For the purpose of publishing, the Security Target [5] 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

CBC Cipher Block Chaining

CC Common Criteria for IT Security Evaluation

CCRA Common Criteria Recognition Arrangement

CEM Common Methodology for Information Technology Security Evaluation

CMAC	Cryptographic Message Authentication Code
cPP	Collaborative Protection Profile
CSPL	Cryptographic Service Provider Light
DRG	Deterministic RNG
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECDHE	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA-EG	Elliptic Curve ElGamal Key Agreement
EMSA-PSS	Encoding Method for Signature Appendix, Probabilistic Signature Scheme
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
ICAO	International Civil Aviation Organization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman cryptosystem
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UCP	Update Code Package

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.

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 (CC)
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html
CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM)
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licensing (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] Security Target BSI-DSZ-CC-1153-V5-2025, Document Version 1.4.5, 02.06.2025, Security Target fiskaly Cloud Crypto Service Provider, fiskaly GmbH

[6] Evaluation Technical Report, Version 6.6, 23.06.2025, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH, (confidential document)

[7] Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Version 1.0, 26 February 2020, BSI-CC-PP-0113-2020

[8] Configuration list for the TOE, SHA256: 98214fe12fadfb8b3622789d16e12f9f4d7c4b3d468650e7dcd0f48caafec442, 20.06.2025, CSPL-v1.5.0_CL-2025-06-20.csv (confidential document)

[9] Guidance documentation for the TOE, Document Version 1.5.1, 20.01.2025, Preparative Procedures & Operational User Guidance Documentation

[10] [FIPS180-4] Secure Hash Standard (SHS) (FIPS 180-4), 04.08.2015, NIST

[FIPS186-4] Digital Signature Standard (DSS) (FIPS 186-4), 19.07.2013, NIST

[FIPS197] Advanced Encryption Standard (AES) (FIPS PUB 197), 26.11.2001, NIST

[ICAO-9303-11] Doc 9303, Machine Readable Travel Documents Part 11 — Security Mechanisms for MRTDs, Seventh Edition, 2015, ICAO

[ISO10116] Information technology — Security techniques — Modes of operation for an n-bit block cipher (ISO/IEC 10116:2017), Edition 4, Juli 2017, ISO

[ISO14888-2] Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms (ISO/IEC 14888-2:2008), Edition 2, April 2008, ISO

[ISO18033-3] Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers (ISO/IEC 18033-3:2010), Edition 2, December 2010, ISO

[7] specifically

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 19, Version 9, Gliederung des ETR
- 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
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[RFC8017] PKCS #1: RSA Cryptography Specifications Version 2.2 (RFC 8017), November 2016, Kathleen Moriarty and Burt Kaliski and Jakob Jonsson and Andreas Rusch

[SP800-38A] Recommendation for Block Cipher Modes of Operation Methods and Techniques (SP 800-38A), 01.12.2001, NIST

[SP800-38B] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication (SP 800-38B), 01.05.2005, NIST

[SP800-38D] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (SP 800-38D), 28.11.2007, NIST

[SP800-38F] Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping (SP 800-38F), 13.12.2012, NIST

[SP800-56C] Recommendation for Key Derivation through Extraction-then-Expansion (SP 800-56C), 28.11.2011, NIST

[SP800-90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators (SP 800-90A Rev. 1), 24.06.2015, NIST

[TR-03110-2] Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS) (TR-03110-2), Version 2.21, 21.12.2016, BSI

[TR-03111] Elliptic Curve Cryptography (TR-03111), Version 2.10, 01.06.2018, BSI

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report