Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1153-V3-2021

for

fiskaly Cloud Crypto Service Provider, Version 1.3.0

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-V3-2021 (*)

Cryptographic Service Provider Light

fiskaly Cloud Crypto Service Provider, Version 1.3.0

from	fiskaly GmbH
PP Conformance:	Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019, Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au) Version 1.0, 26 February 2020, BSI-CC-PP-0112-2020, 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

SOGIS
Recognition Agreement

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 and ALC_FLR
only

Bonn, 17 December 2021

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

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....6

1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9

B. Certification Results....10

1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....13
4. Assumptions and Clarification of Scope....14
5. Architectural Information....14
6. Documentation....16
7. IT Product Testing....16
8. Evaluated Configuration....17
9. Results of the Evaluation....18
10. Obligations and Notes for the Usage of the TOE....20
11. Security Target....21
12. Regulation specific aspects (eIDAS, QES)....21
13. Definitions....21
14. Bibliography....23

C. Excerpts from the Criteria....25

D. Annexes....26

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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[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), 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.

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

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 1.3.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1153-V2-2021. Specific results from the evaluation process BSI-DSZ-CC-1153-V2-2021 were re-used.

The evaluation of the product fiskaly Cloud Crypto Service Provider, Version 1.3.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 3 September 2021. SRC 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 December 2021 is valid until 16 December 2026. 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 1.3.0 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
Mariahilfer Straße 36/5
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 1.3.0. It is a Cryptographic Service Provider Light (CSPLight) claiming the following Common Criteria Protection Profiles:

- Cryptographic Service Provider Light, Version 1.0, registered under BSI-CC-PP-0111-2019, Federal Office for Information Security, 12 November 2019

in combination with the following PP-Modules:

- Protection Profile-Module CSPLight Time Stamp Service and Audit, registered under BSI-CC-PP-0112-2020, Federal Office for Information Security, 26 February 2020
- Protection Profile-Module CSPLight Time Stamp Service and Audit – Clustering, Version 1.0, registered under BSI-CC-PP-0113-2020, Federal Office for Information Security, 26 February 2020

The TOE is a pure Software TOE provided as a Java application. It is intended to be used with products requiring a certified Cryptographic Service Provider Light.

The TOE runs on a PrimeKey SEE hardware platform. As the TOE is a software only product, the hardware was not part of the evaluation. A list of further requirements can be found in chapter 8.

The Security Target [6] is the basis for this certification. It is based on the above mentioned certified Common Criteria Protection Profiles [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_CMS.3, ALC_LCD.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], 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	The TOE provides a cryptographically protected trusted

channel	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
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 secure local trusted Network Time Protocol (NTP) Server.
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 [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], chapters 3.4, 3.2 and 3.3 respectively.

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 1.3.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Software as JAR file: cspl.jar	Version 1.3.0 The TOE is delivered with the accompanying detached signature file cspl.jar.minisig which is provided by fiskaly GmbH. 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]: RWRUupxsFLBrtFlb7g2ZWVFSQE23BvMEtPszqNu2E8Q32U4L99AKexpl.	Physical delivery: Initial signed TOE will be delivered and installed onto the customer's hardware platform via a fiskaly GmbH representative.
2	DOC	Associated guidance documentation: Preparative Procedures & Operational User Guidance Documentation fiskaly Cloud Crypto Service Provider, TOE Version 1.3.0	Version: 1.3.3, Date: 28 July 2021 SHA256: 10D88866AE583C734D7062A32ECADF9913F6B6729FE492D33B8FBC597693292E	Google Cloud storage download and E-Mail

Table 2: Deliverables of the TOE

The TOE is delivered internally by a fiskaly GmbH representative to another fiskaly GmbH representative. After acceptance, the customer installs the TOE on the hardware platform according to the preparative procedures. The guidance documentation is distributed by Google Cloud storage download and E-Mail. All deliverables are signed by the developer who describes the verification procedure in [6], chapter "Code and Document Signing".

An Attestation Key pair to attest the TOE as genuine certified product is delivered via the same method as the TOE itself. Its installation procedure is described alongside the TOE's in [10], chapter 2.3.2.

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:

- authentication of users,
- authentication and attestation of the TOE to entities,
- data authentication and non-repudiation including time stamps,
- encryption and decryption of user data,
- trusted channel functionality,
- management of cryptographic keys,
- generation of random bits,
- time service, time stamp service,
- secure auditing functionality and

- clustering.

Specific details concerning the above mentioned security policies can be found in chapter 7 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 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 [6], chapter 4.2.

5. Architectural Information

The TOE is a software TOE running on dedicated non-TOE hardware (PrimeKey SEE server) as well as dedicated non-TOE software (Alpine Linux, JVM), building the non-TOE platform. The TOE is operated on a hardware platform, namely “PrimeKey SEE”, which is certified according to FIPS 140-2 Level 3. The non-TOE PrimeKey SEE 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

Server 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.

Cryptographic Subsystem

The cryptographic subsystem provides the following functionality to the server subsystem:

- Hash generation for 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. TOE test configuration

The tests were performed on a test system running two virtual machines, the TOE VM and the Testing VM operated at the developer's site. The tested TOE version was 1.3.0.

For testing, the TOE was running on a hardware platform different from chapter 8 and 5. The RNG seed was created on the PrimeKey SEE and manually transferred into the testing environment. After reviewing the architecture and development documentation of the TOE as well as the PrimeKey SEE's hardware documentation, this approach was deemed sufficient for testing in this particular evaluation.

The configuration respectively the version of the TOE can be retrieved from the test environment via the test function `version.request`. It was verified that the tested version 1.3.0 of the TOE is compliant with the provided documentation.

7.2. Testing approach and coverage

Developer Testing

The developer created a suite of tests which can be categorized into three groups: unit tests, TSFI tests an manual tests. These amount to 3107 automated tests and 6 manual tests covering all interfaces and the random number generator of the underlying hardware platform.

The automated tests require no interaction after starting. For manual tests, manual steps like disconnecting the TOE from the network via unplugging need to be performed when prompted.

All test cases were executed successfully by the developer and ended up with the expected result.

Independent Testing

The developer provided access to a preconfigured test environment to the ITSEF. During a dedicated workshop, the developer presented the installation of the test environment using the TOE's guidance documentation.

For independent testing, the ITSEF repeated all developer tests. In addition, some tests were repeated with changed parameters. The entropy of random numbers was tested using the SP-800-90B entropy assessment tool. The evaluators determined that all tests were executed successfully.

7.3. Penetration Testing

For penetration testing, the same environment was used as for independent testing. 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.

Vulnerability Analysis Approach

The evaluator devised an attack scenario exploitable in the TOE's operational environment by an attacker with the attack potential "Basic".

Vulnerability Analysis Verdict

The TOE is resistant against attacks with basic attack potential.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- fiskaly Cloud Crypto Service Provider Version 1.3.0
- Associated guidance documentation: Preparative Procedures & Operational User Guidance Documentation fiskaly Cloud Crypto Service Provider, TOE Version 1.3.0, Version 1.3.3 [10]

For the non-TOE software platform:

- Alpine Linux 3.12.0
- OpenJDK 11 as provided by Alpine Linux
- Busybox 1.31.1

The non-TOE hardware platform is a PrimeKey SEE.

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.

For RNG assessment the scheme interpretations AIS 20 was 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-V2-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the key deletion functionality which is now accessible for the owner of the key to be deleted.

The evaluation has confirmed:

- PP Conformance: Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019,
  Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au) Version 1.0, 26 February 2020, BSI-CC-PP-0112-2020,
  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]
- 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 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. Each Cryptographic Functionality achieves a security level of at least 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Hashing	SHA-256, SHA-384, SHA-512	FIPS 180-4	none	
2	Random Number Generation	RNG	NIST SP-800-90A R1; DRG.3	≥ 125 bits of entropy	Seed length 256 bits
3	Key Generation	AES	ISO 18033-3, NIST SP800-56C	128, 256	
4	Key Derivation	AES	NIST SP800-56C	128, 256	
5	Key Generation	ECC Curve P-256	FIPS PUB 186-4 B.4 and D.1.2.3	256	
6	Key Derivation	ECC Curve P-256 with X9.63 Key Derivation Function	FIPS PUB 186-4 B.4 and D.1.2.374, TR-03111 (Section 4.3.3)	256	
7	Key Generation	RSA	PKCS #1 v2.2	4096	
8	Key Agreement	ECDHE Curve P-256 and 256-bit random ECP group	TR-03111	128, 256	
9	Key Derivation	ECKA-EG Curve P-256 with X9.63 Key Derivation Function	TR-03111, chapter 4.3.2.2	128, 256	
10	Key Generation	ECKA-EG Curve P-256	FIPS PUB 186-4 B.4 and D.1.2.3	256	
11	Key Generation	AES-RSA Key generation and RSA encryption	ISO/IEC18033-3, PKCS #1 v2.2	128, 256	
12	Key Derivation	AES-RSA key derivation and decryption	ISO/IEC 14888-2	128, 256	
13	Key Wrapping	AES Key Wrap with padding	NIST SP800-38F	128, 256	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
14	Confidentiality Protection	AES in CBC mode	NIST SP800-38A, ISO 18033-3, ISO 10116	128, 256	
15	Confidentiality with MAC	AES in CBC mode with CMAC	NIST SP800-38A, NIST SP800-38B	128, 256	
16	MAC	AES with CMAC	NIST SP800-38B	128, 256	
17	Digital Signatures	ECDSA Curve P-256	FIPS PUB 186-4 B.4 and D.1.2.3	256	
18	Digital Signatures	RSA and EMSA-PSS	ISO/IEC 14888-2, PKCS#1, v2.2	4096	
19	Trusted Channel	Chip Authentication Version 2	TR-03110, section 3.3 and 3.4	128, 256	
20	Trusted Channel	Terminal Authentication Version 2	TR-03110, section 3.3 and 3.4	128, 256	
21	Trusted Channel	PACE Curve P-256	ICAO Doc9303, Part 11, section 4.4	128, 256	
22	Trusted Channel	AES in CBC mode	NIST SP800-38A, FIPS197	128, 256	
23	Trusted Channel	AES CMAC	NIST SP800-38B, FIPS197	128, 256	

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 [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

ACPI	Advanced Configuration and Power Interface
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
CCRA	Common Criteria Recognition Arrangement
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CMAC	Cryprographic Message Authentication Code
cPP	Collaborative Protection Profile
CSPLight	Cryptographic Service Provider Light
DHCP	Dynamic Host Control Protocol
DRG	Deterministic RNG
EAL	Evaluation Assurance Level
ECC	Elliptic-curve cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDHE	Elliptic-Curve Diffie–Hellman
EMSA-PSS	Encoding Method for Signature Appendix, Probabilistic Signature Scheme
ECKA-EG	Elliptic Curve ElGamal Key Agreement
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
ICAO	International Civil Aviation Organization

IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JAR	Java Archive
JVM	Java Virtual Machine
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMAERS	Security Module Application for Electronic Record-keeping Systems
SQL	Simple Query Language
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TR	Technische Richtlinie
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.

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-1153-V3-2021, Version 1.2.3, 9 July 2021, Security Target fiskaly Cloud Crypto Service Provider, fiskaly GmbH

[7] Evaluation Technical Report, Version 3.2, 23 August 2021, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH (confidential document)

[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

[8] Base-PP: Protection Profile Cryptographic Service Provider Light (CSPL) Version1.0, 12. November 2019, BSI-CC-PP-0111-2019, BSI

PP-Configuration: Common Criteria Protection Profile Configuration CryptographicService Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au)Version 1.0, 26 February 2020, BSI-CC-PP-0112-2020, BSI

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

[9] Configuration list for the TOE, Version 1.3.0, provided on 27 August 2021, CL_CSPL_1.3.0.zip, SHA256: 933A9478025A93D5AE3BD4C4A19587FFA0716A0FE3EDC5A5AAFFE8EA2B275EC0 (confidential document)

[10] Guidance documentation for the TOE, Version 1.3.3, 28 July 2021, Preparative Procedures & Operational User Guidance Documentation fiskaly Cloud Crypto Service Provider TOE version 1.3.0, fiskaly GmbH

C. Excerpts from the Criteria

[1] 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