Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1139-V4-2024

for

D-TRUST Web-Dienst TSE-CSP, Version 1.4.1

from

D-Trust 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-1139-V4-2024 (*)

CSPL

D-TRUST Web-Dienst TSE-CSP, Version 1.4.1

from	D-Trust GmbH
PP Conformance:	Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_CMS.3 and ALC_LCD.1
valid until:	12 February 2029

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, 13 February 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

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....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....13
5. Architectural Information....14
6. Documentation....14
7. IT Product Testing....14
8. Evaluated Configuration....16
9. Results of the Evaluation....17
10. Obligations and Notes for the Usage of the TOE....18
11. Security Target....18
12. Regulation specific aspects (eIDAS, QES)....18
13. Definitions....18
14. Bibliography....20
C. Excerpts from the Criteria....22
D. Annexes....23

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 und für Heimat (Federal Ministry of the Interior and Community)
- 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.

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 Bundesministerium des Innern und für Heimat 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 D-TRUST Web-Dienst TSE-CSP, Version 1.4.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1139-V3-2021. Specific results from the evaluation process BSI-DSZ-CC-1139-V3-2021 were re-used.

The evaluation of the product D-TRUST Web-Dienst TSE-CSP, Version 1.4.1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 February 2024. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: D-Trust GmbH.

The product was developed by: D-Trust 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 13 February 2024 is valid until 12 February 2029. 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 D-TRUST Web-Dienst TSE-CSP, Version 1.4.1 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] D-Trust GmbH
Kommandantenstr. 15
10969 Berlin
Deutschland

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 named D-TRUST Web-Dienst TSE-CSP and was evaluated in version 1.4.1. The TOE is a pure software TOE and is provided as a Java application. The TOE provides the functionality of a Cryptographic Service Provider (Light).

The TOE does not provide any kind of interface for direct user interaction. Instead, the TOE provides its services in form of RESTful service interfaces based on the HTTP/HTTPS protocol to be consumed by other applications.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles listed in [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 and ALC_LCD.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 10. 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
Self Testing and Integrity Protection
User Identification and Authentication
Access Control
Trusted Channel
Log Message creation and verification
Timestamp and Audit
Management of Certificates
Cryptographic Support
TOE Redundancy and Fail-Over Concept
TOE Secure Update

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 11.

The assets to be protected by the TOE are defined in the Security Target [6], chapters 5.1, 6.1 and 7.1. 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 5, 6 and 7.

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:

D-TRUST Web-Dienst TSE-CSP, Version 1.4.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release / Version	Form of Delivery
1.	SW	Software library as JAR file: csplight-1.4.1-1856182-jar-with-dependencies.jar	SHA-256 hash-value: 1f27366c592f4279073d5e26135379709323668bf611ef90fd80d41d2f28645	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.
2.	DOC	D-TRUST-TSE-WEB DOKUMENTATION UND INTEGRATORHANDBUCH – CSP LIGHT MODUL [10]	Version 1.4.2	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.
3.	DOC	D-TRUST-TSE-WEB SCHNITTSTELLEN- UND FUNKTIONSSPEZIFIKATION CSP-LIGHT-MODUL [11]	Version 1.6.8	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.
4.	DATA	Initial passwords of system users (Administrator, Timekeeper and Auditor-Manager)	-	Personal delivery.

Table 2: Deliverables of the TOE

The TOE deliverables are identified by their individual hash value using SHA-256 or the version number as delivered from the TOE-developer Bundesdruckerei Gruppe GmbH to the applicant D-Trust either via personal delivery, encrypted and signed mail or via a secure download portal. All TOE deliverables are signed by Bundesdruckerei Gruppe GmbH.

The unique hash values or version numbers of the TOE deliverables are stated in Table 2 above. The name and version of the TOE can also be checked by the response to the function GenerateAttestation as described in [11], chap. 5.24.

Similarly, the Integration-, configuration and operations manual [10] and the interface definition [11] are delivered either by personal delivery, encrypted and signed mail or via a secure download portal. All deliverables are signed by the developer. The initial password for system users are only delivered via verbal, personal delivery and are not written down in a document.

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,
- Authentication and attestation of the TOE, trusted channel,
- User identification and authentication,
- Access control,
- Security management,
- Protection of the TSF,
- Import and verification of Update Code Package,
- Time stamp,
- Access control on time stamp service,
- Security Audit, and
- Clustering.

Specific details concerning the above mentioned security policies can be found in Chapters 10.1, 10.2 and 10.3 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,
- OE.AppComp,
- OE.SecManag,
- OE.SecComm,
- OE.SUCP,
- OE.SecPlatform,
- OE.Audit,
- OE.TimeSource,
- OE.ClusterCtrl, and
- OE.TSFdataTrans.

Details can be found in the Security Target [6], chapter 8.2.

5. Architectural Information

The TOE consists of the following subsystems:

- Client Remote Interface: This subsystem provides the endpoint of the trusted channel connection to the client remote entity and realizes the TSFI_Client (Client Remote Interface).
- Administration Interface: This subsystem provides the Administration Interface which is an endpoint of the trusted channel connection to an administrator and realizes the TSFI_Admin (Administration Interface). The Administration Interface provides management and configuration functionality to the owner's (administrator's) client remote entity.
- Seed: This Subsystem utilizes the RNG provided by the HW environment for Seed generation.
- Cryptocore: This subsystem provides the cryptographic functionality of the TOE by utilizing the subsystem Bouncy Castle. It provides the functionality for key generation, hash calculation, trusted channel, signature generation and verification as well as en- and decryption operations.
- Bouncy Castle: This subsystem implements the cryptographic base functionality and provides it to the subsystem Cryptocore for the cryptographic operations.
- Datenverwaltung: This subsystem implements the management functionality for internal and cryptographic data of the TOE.
- Relocate/Failover: This subsystem implements functionality for clustering, such as export and import functionality.
- Update-Time: This subsystem implements the update functionality for the internal system time utilizing the subsystem Update-Time-Application.
- Update-Time-Application: This subsystem implements the functionality for setting the system time.

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

Developer's Test according to ATE_FUN

TOE Configuration:

The TOE was tested in the one and only configuration, which has been executed on Java runtime from OpenJDK 17.

Testing approach:

The tests are performed as Unit tests in the development tool. The developer considered the following aspects when designing his test approach:

- Tests to cover all actions and interfaces defined in [11],
- Good case and bad case tests for each function defined in the document [11] and executable on the TOE, and
- Tests of the cryptographic functionality by test vectors.

Test Results:

All test cases were run successfully on this TOE version.

The developer's testing results demonstrate that the TOE operates as expected.

Independent Testing according to ATE_IND

TOE Configuration:

The TOE was tested in the one and only configuration which can be executed in the Java runtime from OpenJDK 17. All developer tests were repeated by the evaluation body with the final TOE and all independent tests were performed by the evaluation body with the final TOE version 1.4.1.

The keys and personalization data used in the test configuration were provided by the developer.

Testing approach and Setup:

The evaluator tested all TSF using a series of test cases where each test case tests a specific aspect of the expected behaviour. The TSF is mainly tested by running test scripts within the test environment at the TOE interface using the commands defined in [11]. The TSF is stimulated within the test scripts and the behaviour is observed as return value of the TOE.

The tests are performed by test tools which use scripts. Test attributes, preconditions and post processing steps that are coded into the scripts ensure that the script execution is reproducible. The test environment was provided by the developer and the test scripts were implemented by the evaluator.

The selected tests cover tests of the TSFIs related to all TOE Security Functionalities given in Table 1 above and preparative procedures, performed by the evaluator according to the guidance [10] and [11].

Test Results:

The test reports are mainly automatically generated by the test tool used. If several manual test steps are required, the evaluator created a log file.

The test logs and the test documentation include details and comments on the test configuration, on the test equipment used, on the used command structure and the expected results. The test prerequisites, test steps, and expected results adequately test the related TSFIs, and they are consistent with the descriptions of the TSFIs in the functional specification.

The test results have not shown any deviations between the expected test results and the actual test results.

Penetration Testing according to AVA_VAN

Overview:

The penetration testing was performed at the site of the evaluation body TÜVIT with a test environment provided by the sponsor and by the developer on a dedicated test server set

up by the developer. The samples were provided by the developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation.

TOE Configuration:

The TOE was tested in the compiled configuration which runs in the runtime environment on the platform defined in [6] in scope of the certification.

Testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within vulnerability analysis evaluation report, the evaluator created attack scenarios for the penetration tests, where the evaluator is of the opinion that the vulnerabilities could be exploitable. While doing so, the evaluator also considered all aspects of the security architecture of the TOE being not covered by the functional developer tests.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised.

Test Results:

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 of Basic was actually successful in the TOE's operational environment as defined in the security target provided that all measures required by the developer are applied.

Summary of all above mentioned Test Results

The test results yielded 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 [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE needs to run on one of the following hardware platforms:

- PrimeKey SEE Platform ("Secure Execution Environment") of the company "PrimeKey Labs GmbH". The overall product version 1.2.2 includes the TAs (Trust Anchor) firmware version 1.0.2 (FIPS certified) and the hardware version 1.0.0 (FIPS certified). This product provides an interface ("SEE Loader", certified to FIPS 140-2 Level 3) through which the required TOE software is deployed.
- Enforcer R2 of the company "private machines". The R2 version includes the hardware version ENFORCER.R2.X12SDV.1.0.0 and the following software/firmware versions: Security Anchor Bootloader 1.0.0, Security Anchor Firmware 1.4.0, libdrbg: 1.0.2, libucl: 2.5.13, Compute Engine Firmware: 1.0.0, Compute Engine Application 1.0.0, Compute Engine PM FIPS Crypto Library: 1.0.0.

There is one configuration of the TOE which requires one of two specified HW-platforms comprising a Java Virtual Machine, a particular operating system and a dedicated hardware. For all tests the TOE is configured and parametrized, if necessary, according to the guidance documents.

The TOE needs to be installed according to the guidelines given in [10] and [11] and requires a specified platform as defined in [6], chap. 2.8, and an operational environment as defined in [6], chap 2.9.

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_CMS.3 and 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-1139-V3-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was a new HW platform, minor bug fixes and improvements to the TOE, for more detail see [12].

The evaluation has confirmed:

- PP Conformance: Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019 and two PP-Modules BSI-CC-PP-0112-2020 and BSI-CC-PP-0113-2020, see [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 and 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 table presented in chapter 3.5 of the Security Target [6] gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its

rating from cryptographic point of view. In this table, each Cryptographic Functionality achieves a security level of at least 100 Bits (in general context).

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

AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
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
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

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HW	Hardware
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
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TC	Trusted Channel
TOE	Target of Evaluation
TSE	Technische Sicherheitseinrichtung
TSF	TOE Security Functionality
TSFI	TSF Interfaces
TSS	Technical Security System (CSPL-Kontext)
TSS	TOE Summary Specification (CC-Kontext)

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-1139-V4-2024, Version 1.4.5, 26 January 2024, D-TRUST Web-Dienst TSE-CSP Security Target, D-TRUST GmbH

[7] Evaluation Technical Report, Version 4, 26 January 2024, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH – Evaluation Body for IT Security, (confidential document)

[8] Base-PP: Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019, BSI

PP-Module: 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, BSI

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 41, Version 2, Guidelines for PPs and STs
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

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

[9] Configuration list consisting of:

D-TRUST Web-Dienst TSE-CSP - Referenzliste, Version 2.3.4, 26 January 2024, D-TRUST GmbH

List of all files of the git repository, files-csp.txt, D-TRUST GmbH, SHA-256-value: bab6aebf14a5fd6423b43cbdf6e70eaed3ae8bfc1ae8c6072138a1364be5a45a

[10] D-TRUST-TSE-WEB DOKUMENTATION UND INTEGRATORHANDBUCH – CSP LIGHT MODUL, Version 1.4.2, 26 January 2024, D-TRUST GmbH

[11] D-TRUST-TSE-WEB SCHNITTSTELLEN- UND FUNKTIONSSPEZIFIKATION CSP-LIGHT-MODUL, Version 1.6.8, 08 November 2023, D-TRUST GmbH

[12] [IAR], D-TRUST-TSE-WEB AUSWIRKUNGSANALYSE D-TRUST WEB-DIENST TSE-CSP, Version 1.0.0, 2022-07-15, D-TRUST GmbH

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