Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1145-2021

for

CryptoServer CSPLight Version 1.0.0

from

Utimaco IS 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-1145-2021 (*)

Cryprographic Service Provider Light

CryptoServer CSPLight, Version 1.0.0

from	Utimaco IS 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 and ALC_LCD.1

SOGIS
Recognition Agreement

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, 1 April 2021

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- 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 CryptoServer CSPLight, Version 1.0.0 has undergone the certification procedure at BSI.

The evaluation of the product CryptoServer CSPLight, Version 1.0.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 25 March 2021. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Utimaco IS 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 1 April 2021 is valid until 31 March 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 Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

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 CryptoServer CSPLight, Version 1.0.0 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] Utimaco IS GmbH
Germanusstraße 4
52080 Aachen

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 Utimaco CryptoServer CSPLight, Version 1.0.0. It is a Cryptographic Service Provider Light (CSPLight) claiming the Common Criteria Protection Profile Cryptographic Service Provider Light – Time Stamp And Audit – Clustering (PPC-CSPLight-TS-Au-Cl). The TOE is a pure Software Product consisting of a Java application and firmware for the Hardware Security Module. It is intended to be used with products requiring a certified Cryptographic Service Provider Light.

The TOE runs on the CryptoServer CSPLight server platform which includes a Hardware Security Module (HSM). As the TOE is a pure software product, the hardware was not part of the evaluation.

The non-TOE software is installed by Utimaco on the dedicated non-TOE Hardware. The software itself is outside of the TOE Scope but can be updated via Utimacos own RPM package repository as described in [12] section 2.2.1.5

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile 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].

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] and [9], chapter 7.They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.]

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

TOE Security Functionality	Addressed issue
SF.USER_AUTH: User Authentication	The TOE provides user authentication. The use of any of the security-relevant services of the TOE is not possible without user authentication.
SF.TRUSTED_CHANNEL: Trusted Channel	The TOE supports to establish a cryptographically protected trusted channel between the TOE and external entities.
SF.ATTESTATION: Authentication and Attestation of the TOE	TOE samples are delivered with attestation keys to attest these samples as genuine certified products. Attestation of the TOE's identity to external entities is part of establishing trusted channels like PACE, terminal authentication or chip authentication.

TOE Security Functionality	Addressed issue
SF.CRYPTO: Cryptographic Support	The TOE's security function provides cryptographic support for the other TSFs using cryptographic mechanisms, and it enables cryptographic services like signature generation and verification for the user and provides key derivation services for internal purposes.
SF.ADMIN: Administration	The TOE provides functionality to administrate itself in a secure and controlled way, via its security function provides access control on cryptographic TSF and cryptographic keys using also the internal cryptographic services.
SF.KEY_MAN: Key Management	The Key Management of the TOE covers the security functionality related to management of cryptographic keys with security attributes including key generation, key derivation and key agreement, internal storage of keys, import and export of keys with protection of their confidentiality and integrity.
SF.SWUPDATE: Software Update	The TOE security function supports downloading, integrity and authenticity verification and decryption of Update Code Packages (UCP) for the CryptoServer CSPLight.
SF.CLUSTER: Clustering of the TOE	The TOE provides functionality to establish a cluster of TOE samples for scalability of performance and availability of security services.
SF.TIMESTAMP: Time Stamp Service	The TOE provides a time service as well as a time stamp service.
SF.AUDIT: Audit	The TOE provides secure auditing functionality which generates audit records on selected user activities and security events of the TOE.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1. 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] and [9], chapters 4.5, 4.3 and 4.4, 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:

CryptoServer CSPLight, Version 1.0.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	CryptoServer CSPLight	Version 1.0.0	Preinstalled on the dedicated non-TOE CryptoServer CSPLight Server platform delivered via a shipping company from the developer production to the customer
2	DOC	CryptoServer CSPLight Betriebsanleitung [11] SHA256: 780A033D7DADB557DADFAB8324F8494AD6E4AE317D49F6076DC0B5A67FFA4EF1	2021-03-18 Version 1.0.1	Delivered on a CD-ROM together with the TOE
3	DOC	CryptoServer CSPLight Administration Manual [12] SHA256: AE9927ED5923806A9538AD007109FE504B010D01A36481CBECDC08FBF7323119	2021-03-17 Version 1.0.0	Delivered on a CD-ROM together with the TOE
4	DOC	CryptoServer CSPLight Clustering API SHA256: A5D97D72A4DA1BA025AE5D0E439E590FAAF8F8D63074C841EBFD260BCDA505E5	2020-11-13 Version 1.4.0	Delivered on a CD-ROM together with the TOE
5	DOC	CryptoServer CSPLight Core API SHA256: F8ECC0414E44288D11E57A695CF8F46E88F2393BF28DEC34FF0469BF72D8D0F6	2020-02-19 Version 1.6.0	Delivered on a CD-ROM together with the TOE
6	DOC	CryptoServer CSPLight Crypto API SHA256: B6C95FF166C1D472BC3FF4FB6BBEA871B0DC51887309B66501B1C022D0D3352A	2020-11-13 Version 1.2.0	Delivered on a CD-ROM together with the TOE
7	DOC	CryptoServer CSPLightUI Logic API SHA256: 137D86EC36A5F2A7273A33667B5C5DB6FCC0F454179B9A93EDEB566D7AB9E5FF	2020-12-17 Version 1.5.0	Delivered on a CD-ROM together with the TOE

Table 2: Deliverables of the TOE

The TOE is delivered preinstalled onto the dedicated non-TOE server platform. This installation is performed during production by the developer Utimaco IS GmbH.

Delivery of sensitive electronic data and guidance documentation is performed via CD-ROM together with the TOE installed on its dedicated non-TOE Server Hardware which contains seals and serial numbers that are unique for each TOE instance.

In parallel, the customer is provided with related delivery information that contain the serial numbers of the delivered Product containing the TOE via E-Mail, which is electronically signed. The authenticity of the key used for signing the E-Mail can be verified by the customer via telephone call with Utimaco IS GmbH.

Further details on TOE verification can be found in the developer’s documentation [11].

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
- clustering

Specific details concerning the above mentioned security policies can be found in chapter 9 of the Security Target [6] and [9].

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
- OE.TSFdataTrans: Transfer of TSF data within the CSPLight cluster

Details can be found in the Security Target [6] and [9], chapter 5.2.

5. Architectural Information

The TOE is a software TOE running preinstalled on dedicated non-TOE hardware as well as dedicated non-TOE software provided by Utimaco. The CryptoServer CSPLight hardware consists of a physically hardened server in which an HSM is additionally installed. The HSM hardware is considered non-TOE while the HSM firmware belongs to the TOE part of the product. A modified version of the HPE ProLiant DL360 Gen9 Server including CryptoServer HSM (in the form of a PCIe card) constitute the hardware of the CryptoServer CSPLight product. The server itself is not TOE but together with its operating system it provides the platform for the TOE software modules.

The SFR-enforcing subsystems of the TOE are:

- CSPLight Core
- CSPLight Clustering
- CSPLight UI Logic
- CSPLight Crypto API
- CSPLight Crypto Services
- CSPLight HSM Firmware

The subsystems provide the following functionality:

User Authentication

The use of any of the security-relevant TSFI services of the TOE is not possible without appropriate user identification & authentication (I&A).

Trusted Channel

Establish a cryptographically protected trusted channel between the TOE and external entities. The application component (in client role) uses the security services of the TOE (in server role). TOE provides PACE protocol in ICC role for the trusted channel to protect the integrity of the messages exchanged.

Authentication and Attestation of the TOE

The attestation keys are generated by the TOE manufacturer and securely imported into the TOE during its production. The published attestation public key can be used to verify i.e. attest that the TOE owns the corresponding private key and is directly linked to the TOE manufacturer as the certified product variant.

Cryptographic Support

Contains all the cryptographic operations required and used by the TOE, in order to be able to fulfil its required functionality. This includes random number generation and the functionalities listed in table 3.

Administration

Provides functionality to administrate itself in a secure and controlled way.

Key Management

Provides security functionality related to management of cryptographic keys with security attributes including key generation, key derivation and key agreement, internal storage of keys, import and export of keys with protection of their confidentiality and integrity.

Software Update via UCP

Supports downloading, integrity and authenticity verification and decryption of Update Code Packages (UCP) for the CryptoServer CSPLight. Only after its successful verification of authenticity and UCP payload decryption, the UCP Payload is stored to proceed with the TOE platform software update procedures.

Clustering of the TOE

Provides security functionality to establish a cluster of TOE samples for scalability of performance and availability of security services via Master-Slave-Cluster-Configuration composed of two TOE samples.

Time Stamp Service

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.

Audit

Provides secure auditing functionality which generates audit records on selected user activities and security events of the TOE. The audit records are generated in the TOE and can be exported to a SMA for further use.

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

Tests are performed on a TOE installed on the real dedicated non-TOE Hardware in a Master-Slave-Cluster-Configuration. The tested TOE version was 1.0.0. For testing, the TOE was running on the dedicated non-TOE hardware platform.

The configuration respectively the version of the TOE can be retrieved from the test environment via the test function **IF_CSPL_UI_LOGIC__getInfo__ok()**. The evaluators verified that the tested version 1.0.0 of the TOE is compliant with the provided documentation.

7.2. Testing approach and coverage

Developer Testing

The tests performed can be categorized into several groups: Unit and TSFI API tests. With the TSFI API tests the developer specified and implemented test cases for each defined TSFI. Thus all TSFIs are covered by several test cases and each SFR-enforcing subsystem is covered by at least one test case.

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 is done by the developer.

The relevant TSFI API tests cover all TSFIs and operations that are externally accessible. Automatic TSFI API tests are implemented as test cases and consist of 350 test cases.

The unit tests are written during development and are executed on the build system automatically and check the low-level implementation of all modules/classes and their methods to verify that these work as designed.

All TSFI API test cases were executed successfully and ended up with the expected result.

Independent Testing

The TOE is placed inside a test environment in the developer premises which provides operational capabilities. During a dedicated workshop the developer presented this testing approach to the ITSEF and the Certification Body.

For independent testing, the ITSEF repeated all developer TSFI API Tests. In addition, some independent evaluator tests were performed that were based on the test suite of the developer.

The overall test result is that no deviations were found between the expected and the actual test results.

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.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- CryptoServer CSPLight (preinstalled on the dedicated non-TOE CryptoServer CSPLight Server Platform)
- The guidance documentation:
  - CryptoServer CSPLight Betriebsanleitung [11]
  - CryptoServer CSPLight Administration Manual [12]
- The Developer Documentation of the TOE REST API:
  - CryptoServer CSPLight Clustering API
  - CryptoServer CSPLight Core API
  - CryptoServer CSPLight Crypto API
  - CryptoServer CSPLight UI-Logic API

The following software constitutes the non-TOE software platform:

- Hypervisor: SUSE Linux Enterprise Server 15 SP1
- 2 Virtual Machines: Leap 15.1 JeOS SuSE Linux System

- JVM Version 1.8.0_242-b08
- nginx: 1.14.0nt
- ntpd (Host): chronyd (chrony) 3.2
- Apache Webserver: Apache 2.4.33-3.15.1
- Apache Tomcat: 9.0.29
- MariaDB: 10.2.29-MariaDB SUSE package
- System Daemon: 3.0.0 (used for all operations that can only be performed by the hypervisor)
- Keepalived: 2.0.19

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 and ALC_LCD.1 augmented for this TOE evaluation.

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 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 in annex B of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. All applicable Cryptographic Functionalities achieve a security level above 100 Bits.

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 [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

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
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	Cryptographic Message Authentication Code
cPP	Collaborative Protection Profile
CSPLight	Cryptographic Service Provider Light
DRG	Deterministic RNG
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorihm
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
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
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.

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-1145-2021, Version 1.0.2, 2021-03-18, Security Target for CryptoServer CSPLight, Utimaco IS GmbH (confidential document)

[7] Evaluation Technical Report, Version 1.5, 2021-03-26, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH (confidential document)

[8] 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

[9] Security Target BSI-DSZ-CC-1145-2021, Version 1.0.2, 2021-03-18, Security Target Lite for CryptoServer CSPLight, Utimaco IS GmbH (sanitised public document)

[10] Configuration list for the TOE, Version 1.0.1, 2021-03-18, CryptoServer CSPLight Configuration Management (confidential document)

[11] Preparative guidance documentation for the TOE, Version 1.0.1, 2021-03-18, CryptoServer CSPLight Betriebsanleitung, Utimaco IS GmbH

[12] Operative guidance documentation for the TOE, Version 1.0.0, 2021-03-17, CryptoServer CSPLight Administration Manual, Utimaco IS GmbH

[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 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

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.

Annex B: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1145-2021

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Authenticity	RSA-signature generation and verification (EMSA-PSS)	ISO/IEC 14888-2, PKCS #1, v2.2	modulus length: 2048, 3072, 4096	FCS_COP.1/CDS-RSA
2	Authenticity	ECDSA-signature generation and verification	RFC5639, TR-03111 section 4.1.3	all key sizes according to the elliptic curves brainpoolP256rl brainpoolP384r1, brainpoolP512r1 Curve P-256 Curve P-384 Curve P-521	FCS_COP.1/CDS-ECDSA
3	Authenticity	Signature verification of the Update Code Package using ECDSA with brainpoolP256r1 and cryptographic key size 256 bits	RFC5639, TR-03111 section 4.1.3	256	FCS_COP.1/VDSUCP
4	Authentication	ECDSA-signature verification	RFC5639, TR-03111 section 4.1.3	all key sizes according to the elliptic curves brainpoolP256rl brainpoolP384r1, brainpoolP512r1 Curve P-256 Curve P-384 Curve P-521	FDP_DAU.2/Att FDP_DAU.2/Sig FDP_DAU.2/TS
5	Key Agreement	ECDHE with parameters: Elliptic curve: brainpoolP256r1 and 256-bit random ECP group with IANA assigned ID value of 19 Key Derivation Function: X9.63	TR-03111 section 4.3.2.1	256 (ECC keys)	FCS_CKM.5.1/ ECDHE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
6	Key Agreement	ECKA-EG with parameters: Elliptic curve: brainpoolP256r1 Key Derivation Function: X9.63	TR-03111 section 4.3.2.2	256 (ECC keys)	FCS_CKM.5/ECKA-EG FCS_CKM.1/ECKA-EG
7	Key Agreement	PACE with brainpoolP256r1 and Generic Mapping in ICC role	ICAO Doc9303 Part 11 section 4.4	256	FIA_API.1/PACE FCS_CKM.1/PACE
8	Key Agreement	Cluster Key Agreement using PACE with generic mapping in ICC role (TOE Master only) and PACE in Terminal role (TOE Slave only) for FCS_CKM.5/CLDH with brainpoolP256r1 ECC curve	TR-03111	256	FCS_CKM.5/CLDH
9	Key Generation	AES key generation using a byte string derived from input parameters with a X9.63 KDF	NIST-SP800-56C	128, 256	FCS_CKM.5/AES
10	Key Generation	ECC Key pair generation with all elliptic curves	RFC5639, TR-03111 section 4.1.3	all key sizes according to the elliptic curves brainpoolP256rl brainpoolP384r1, brainpoolP512r1 Curve P-256 Curve P-384 Curve P-521	FCS_CKM.1/ECC
11	Key Generation	RSA key pair generation	PKCS #1 v2.2	2048, 3072, or 4096 modulus size	FCS_CKM.1/RSA
12	Key Generation	ECC key pair generation with brainpoolP256r1 for Cluster Key Generation	TR-03111 section 4.1.3	256	FCS_CKM.5/CLDH
13	Key Generation	Seed generation for hybrid data encryption/decryption with data integrity	AIS 20 chapter 4.9	256	FCS_CKM.1/ AES_RSA for seed generation

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
14	Key Derivation	AES Key derivation via AES key generation using a bit string derived from input parameters with a X9.63 KDF	NIST-SP800-56C	128, 256	FCS_CKM.1/TCAP
15	Key Derivation	ECC Key pair derivation with the curve: brainpoolP256r1 and ANSI X9.63 Key Derivation Function	RFC5639, TR-03111 section 4.1.3	256	FCS_CKM.5/ECC
16	Confidentiality	AES decryption and encryption with AES in CBC mode	FIPS PUB 197 (AES), NIST-SP800-38A (CBC)	128, 256	FCS_COP.1/ED
17	Confidentiality	Decryption of encrypted Update Code Packages using AES block cipher in CBC mode with PKCS#5 padding	NIST-SP800-38A chapter 6.2, FIPS PUB 197 chapter 5	256	FCS_COP.1/DecUCP
18	Confidentiality	hybrid data encryption and decryption with asymmetric key encryption	NIST-SP800-38A, NIST-SP800-38B, FIPS PUB 197	asymmetric keys 2048, 3072, or 4096 modulus size	FCS_COP.1/HEM FCS_CKM.1/ AES_RSA FCS_COP.1/HDM CS_CKM.5/AES_RSA
19	Confidentiality	Key wrapping and unwrapping with AES-Keywrap	NIST-SP800-38F	128, 256	FCS_COP.1/KW FCS_COP.1/KU
20	Integrity, Authenticity	HMAC with SHA-256	RFC2104 ISO/IEC 9797-2	512	FCS_COP.1/HMAC
21	Integrity, Authenticity	AES CMAC with AES-128 and AES-256	FIPS PUB 197 (AES), NIST-SP800-38A (CBC)	128, 256	FCS_COP.1/MAC
22	Trusted Channel	PACE with brainpoolP256r1 and Generic Mapping in ICC role	ICAO Doc9303 Part 11 section 4.4	256	FIA_API.1/PACE FTP_ITC.1 FCS_CKM.1/PACE FCS_COP.1/TCE FCS_COP.1/TCM

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
23	Trusted Channel	PACE in Terminal role for Cluster Key Agreement	ICAO Doc9303 Part 11 section 4.4	256	FCS_CKM.5/CLDH FCS_COP.1/TCE FCS_COP.1/TCM
24	Trusted Channel	Chip Authentication Version 2	TR-03110 Part 2 section 3.4	256	FCS_CKM.1/TCAP FCS_COP.1/TCE FCS_COP.1/TCM
25	Trusted Channel	Terminal Authentication Version 2	TR-03110 Part 2 section 3.3	256	FCS_CKM.1/TCAP FCS_COP.1/TCE FCS_COP.1/TCM
26	Cryptographic Primitive	Hash SHA-256, SHA-384, SHA-512	FIPS PUB 180-4	n/a	FCS_COP.1/Hash
27	Cryptographic Primitive	Random Number Generation: hybrid deterministic RNG class DRG.4	AIS 20 chapter 4.9	n/a	FCS_RNG.1

Table 3: TOE cryptographic functionality