Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1230-2026

for

SUSE Linux Enterprise Server Version 15 SP7

from

SUSE LLC

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-1230-2026 (*)

Operating System

SUSE Linux Enterprise Server, Version 15 SP7

from	SUSE LLC
PP Conformance:	U.S. Government Approved Protection Profile - Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022, CCEVS-VR-PP-0091, Functional Package for Transport Layer Security (TLS), Version 1.1, 12 Februar 2019, NIAP, Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 extended ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1
valid until:	23 February 2031

SOGIS Recognition Agreement for components up to EAL 4

Common Criteria

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

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), 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.

Bonn, 24 February 2026

For the Federal Office for Information Security

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

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBI. 2025 , no. 301, p. 2

[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 02 December 2025, Bundesgesetzblatt 2025, no. 301

[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 according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the extended component ALC_TSU_EXT.1 which is not mutually recognised in accordance with the provisions of the SOGIS MRA.

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product SUSE Linux Enterprise Server, Version 15 SP7 has undergone the certification procedure at BSI.

The evaluation of the product SUSE Linux Enterprise Server, Version 15 SP7 was conducted by atsec information security GmbH. The evaluation was completed on 23 February 2026. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: SUSE LLC.

The product was developed by: SUSE LLC.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 24 February 2026 is valid until 23 February 2031. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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 SUSE Linux Enterprise Server, Version 15 SP7 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

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

[6] SUSE LLC
1221 S Valley Grove Way
#500, Pleasant Grove, UT 84062
United States

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 SUSE Linux Enterprise Server 15 SP7, a highly-configurable Linux-based operating system that has been developed to provide a good level of security as required in commercial environments.

The Security Target [5] is the basis for this certification. It is based on the certified General Purpose Operating System Protection Profile [7] supplemented by functional packages for SSH [8] and TLS [9].

The TOE Security Assurance Requirements (SAR) relevant for the TOE are outlined in the Security Target [5], chapter 6.3. They are selected from Common Criteria Part 3 and there is one additional Extended Component defined in the Protection Profile. Thus the TOE is CC Part 3 extended. The TOE meets the assurance requirements defined in the Protection Profile.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
Audit	The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified by the requirements. Each audit record contains the date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event.
Cryptographic support	The TOE includes the OpenSSL version 3.1.4 cryptographic libraries for performing userspace cryptographic operations. In addition, the Linux kernel crypto API performs the cryptographic operations performed by the kernel. In addition, the TOE uses software noise sources for entropy generation. The TOE implements TLS for secure communications with remote servers. The TOE implements SSH for allowing secure remote administration.
User data protection	The TOE implements access controls which can be configured to prevent unprivileged users from accessing files and directories owned by other users. The configuration of the access control mechanism is left to the owner of the file system object.
Identification and Authentication	All users, including administrators, must be authenticated to the TOE prior to carrying out any actions, including management operations. The TOE supports password-based authentication, authentication based on SSH-keys, as well as X.509 certificate-based authentication. The TOE will lock out user accounts after a defined number of unsuccessful authentication attempts to that user account has been met.

TOE Security Functionality	Addressed issue
Security Management	The TOE can perform management functions. The administrator has full access to carry-out all management functions offered by the TOE. The user is allowed a limited set of administrative operations for his own user account.
Protection of the TSF	The TOE implements the following protection of TSF data functions. ● Access controls ● Address space layout randomization (ASLR) with 11 bits (stack) and 28 bits (text segment start address) of entropy ● Stack buffer overflow protection ● Verification of integrity of the boot-chain ● Trusted software updates using digital signatures
TOE Access	The TOE displays an advisory warning message regarding unauthorized use of the OS prior to establishment of a user session.
Trusted Path/Channel	The TOE supports TLS v1.2 for trusted channel communications. The TOE uses TLS to securely communicate with the SUSE Customer Center. Applications may invoke the TOE-provided TLS to securely communicate with remote servers. The TOE offers an SSH server which uses the SSHv2 protocol allowing remote administration.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 1.5.2.

The TOE Security Problem Definition has been taken from the Protection Profile [7] and is defined in terms of Threats and Assumptions. This is outlined in the Security Target [5], chapter 3.1 resp. 3.2.

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 52, 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:

SUSE Linux Enterprise Server, Version 15 SP7

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW (ISO)	SLE-15-SP7-Full-x86_64-GM-Media1.iso SHA256: cd9430420726219f9c73aa7a389b43057e1d9c610d279b7f71d3687c06d8e66c	SLES 15 SP7	download
2	SW (ISO)	SLE-15-SP7-Full-aarch64-GM-Media1.iso SHA256: 9a136f0bff5473e82ec1ebe34e8fbac1bdc0cdfd128b3219b4e2ab2df6654d44)	SLES 15 SP7	download
3	SW (ISO)	SLE-15-SP7-Full-s390x-GM-Media1.iso SHA256: 052b4627a811afd39d9ae27da5727364760b9ea6159fc0848d0600b4419d1f23	SLES 15 SP7	download
4	DOC	Common Criteria Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP7 SHA256: 72b494f5426edac14607229e138aa278cfbb446641337caec9a1c2b41fa530fe	SLES 15 SP7, Document version 1.0	download
5	rpm	openssh	9.6p1-150600.6.34.1	download and verification by the TOE
6	rpm	openssh-client	9.6p1-150600.6.34.1	download and verification by the TOE
7	rpm	openssh-common	9.6p1-150600.6.34.1	download and verification by the TOE
8	rpm	openssh-helpers	9.6p1-150600.6.34.1	download and verification by the TOE
9	rpm	openssh-server	9.6p1-150600.6.34.1	download and verification by the TOE
10	rpm	kernel-default	6.4.0-150700.53.22.1	download and verification by the TOE
11	rpm	audit-audispd-plugin	3.0.6-150400.4.16.1	download and verification by the TOE
12	rpm	yast2-online-update	4.7.0-150700.1.1	download and verification by the TOE
13	rpm	yast2-online-update-configuration	4.7.0-150700.1.1	download and verification by the TOE
14	rpm	firewalld	2.0.1-150600.3.5.1	download and verification by the TOE

Table 2: Deliverables of the TOE

The delivery of the TOE is via electronic download only in the form of ISO images and additional rpm packages. The packages that make up the TOE are digitally signed using OpenPGP/GnuPG. The key of the developer is contained on the installation ISO, as described in the Evaluated Configuration Guide [11].

The developer provides and operates the download site and provides checksums for the downloaded images that enable the user to verify the integrity of the download.

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: Security audit, Cryptographic

support, User data protection, Identification and authentication, Security Management, Protection of the TSF, TOE Access and Trusted Path/Channels.

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:

- The OS relies on being installed on trusted hardware. (OE.PLATFORM)
- The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use. (OE.PROPER_USER)
- The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy. (OE.PROPER_ADMIN)

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

5. Architectural Information

SUSE Linux Enterprise Server (SLES) is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications.

The SLES evaluation covers a potentially distributed network of systems running the evaluated versions and configurations of SLES as well as other peer systems operating within the same management domain. The hardware platforms selected for the evaluation consist of machines, which are available when the evaluation has completed and to remain available for a substantial period of time afterwards.

The TOE Security Functions (TSF) consist of functions of SLES that run in kernel mode plus a set of trusted processes. These are the functions that enforce the security policy as defined in this Security Target. Tools and commands executed in user mode that are used by an administrative user need also to be trusted to manage the system in a secure way. But as with other operating system evaluations they are not considered to be part of this TSF. The hardware, the BIOS firmware and potentially other firmware layers between the hardware and the TOE are considered to be part of the TOE environment.

The TOE includes standard networking applications, including applications allowing access of the TOE via cryptographically protected communication channels, such as SSH and TLS.

System administration tools include the standard command line tools. A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a network server using a port above 1024 may be used as a normal application running without root privileges on top of the TOE. The additional documentation specific for the evaluated configuration provides guidance how to set up such applications on the TOE in a secure way.

6. Documentation

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

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

7. IT Product Testing

The evaluator performed all the tests defined in the Protection Profile (PP) [7] and Functional Packages (FPs) [8][9], which makes it around 100 tests. For the test requirements on cryptographic primitives and RNG, the ACVP tests were performed on all applicable cryptographic algorithms.

Test approach

The evaluator followed the test requirements from the PP and FPs and constructed the tests. He used the evaluator test plan as an entry point, which explains the test configuration, and links the test requirements (including the complete text specification from the PP and FPs), to the actual test procedure.

The evaluator tests are partly manual tests, and partly automated.

Test configuration

The evaluator verified the correctly set up test systems according to the documentation in the Evaluated Configuration Guide and the test plan.

The evaluator tested on hardware setup defined in the Security Target [5]. See also Chapter 8 for details.

All tests were performed on all hardware platforms.

The evaluator executed tests on the TOE, most notably kernel version 6.4.0-150700.53.22.1 for Intel, AMD, z16 , and ARM.

Test Depth

Two types of tests were performed - independent testing as defined by the PP and FPs as well as CAVS algorithm testing:

Independent Testing

The tests mainly comprised of tests that test the external interfaces, but there were also tests that target TOE security behavior that is normally hidden from the outside:

- stack protection: a tool has been used that analyses the binary file meta data to determine whether stack protection is enforced
- binary modifications: for integrity/boot tests the kernel or program packages where modified
- adapted TLS and SSH servers/clients: modified versions of TLS/SSH peers were used to force protocol misbehavior as mandated by the PP and FPs

Algorithm Testing

Multiple algorithm testing is required to be performed by the PP and the FPs. The ACVP parser tool was used to trigger the cryptographic interfaces with the given test vectors for validation.

Results

The TOE platforms showed no deviation from the expected results have been encountered.

8. Evaluated Configuration

This certification covers the following configurations:

The installation of the TOE must be carried out as described in Evaluated Configuration Guide (ECG) [11], which describes the actual installation steps as well as additional configuration steps that need to be carried out when the TOE is installed.

The ECG [11], in section 1.3.1 and the ST [5], in section 1.5.1 also define a number of hardware platforms:

- x86 64bit Intel Cascade Lake processors on Delta D20x-M1-PC-32-8-96GB-1TB-2x1G
- x86 64bit AMD EPYC 3rd Generation processors on Gigabyte R181-Z90
- ARM 64 bit ARMv8.2-A processors on Gigabyte R181-T90
- IBM Z System z16 with TOE executing within an LPAR

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used guidance specific for the technology of the product as present in the Protection Profile [5] and the Functional Packages [8][9].

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

The extended assurance component as defined in the Protection Profile and the Security Target was 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 claimed in the Security Target [5], chapter 6.3 and defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022, CCEVS-VR-PP-0091, NIAP [7]
  Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019, NIAP [8]
  Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP [9]

	Technical Decisions listed in Chapter 2.1 in the Security Target [6]
• for the Functionality:	PP conformant Common Criteria Part 2 extended
• for the Assurance:	Common Criteria Part 3 extended ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.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 52, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The tables in annex B of part D of this report give an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outline its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

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

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

11. Security Target

For the purpose of publishing, the Security Target [5] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

ACVP	Automated Cryptographic Validation Protocol
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
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FP	Functional Package
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
ISO	ISO 9660 filesystem image
PP	Protection Profile
RNG	Random Number Generator
RPM	RPM package manager
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
SSH	Secure Shell
ST	Security Target
SW	Software
TLS	Transport Level Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

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

Informal – Expressed in natural language.

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

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

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

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

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 licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

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

[7] specifically

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

[5] Security Target BSI-DSZ-CC-1230-2026, SUSE Linux Enterprise Server 15 SP7 Security Target, Version 1.0, Date 23 February 2026, Document Title, Developer Name

[6] Evaluation Technical Report, Final Evaluation Technical Report, Version 5, Date 23 February 2026, atsec information security GmbH (confidential document)

[7] Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022, CCEVS-VR-PP-0091, NIAP

[8] Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP

[9] Functional Package for Transport layer Security (TLS), Version 1.1, 01 March 2019, NIAP

[10] Configuration list for the TOE, Master Configuration List, as of 2026-02-23 (confidential document)

[11] Guidance documentation for the TOE, Common Criteria Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP7 (NIAP) – GPOS, Version 1.0, 23 February 2026, SUSE LLC

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-1230-2026

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-2 (rsa-sha2-256 or rsa-sha2-512)	[RFC8017], PKCS#1 v2.2 sec. 8.2(RSA) [FIPS180-4] (SHA) [RFC4253] (SSH-TRANS) for host authentication [RFC4252] sec. 7 (SSH-AUTH) for user authentication [RFC8332] for rsa-sha2-256/512	3072, 4096	Yes	Pubkeys are exchanged trust-worthily out of band, e.g. checking finger-prints. Authenticity is not part of the TOE. (no certificates are used)
2	Authentication	ECDSA signature generation and verification using SHA-{384, 512} on nistp-{, 384, 521} (ecdsa-sha2-nistp384,ecdsa-sha2-nistp521)	[ANSIX9.62] (ECDSA) [FIPS180-4] (SHA) NIST curves [FIPS186-5] identifiers analogous to [RFC5903] sec 5 [RFC5656] secp{384,521}r1 [SEC2] [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	384, 521	Yes	
3	Key agreement	DH with diffie-hellman-group16-sha512, diffie-hellman-group18-sha512 (for RSA)	[RFC4253] (SSH-TRANS) supported by [RFC4419] and [RFC8268] (DH-Group Exchange) [FIPS-180-4] (SHA)	4096, 8192 (prime modulus)	Yes	
4	Key agreement	ECDH with P-384/521 (ecdh-sha2-nistp384, ecdh-sha2-nistp521)	[RFC4253] (SSH-TRANS) [FIPS-180-4] (SHA) supported by	384, 521	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
			[RFC5656] (ECC in SSH) P-384/521 NIST curves [SP800-186]			
5	Confidentiality	AES in GCM mode aes256-gcm-@openssh.com	[FIPS197] (AES), [RFC5647] (SSH-2 using AES with GCM mode)	256	Yes	
6	Integrity and Authenticity	HMAC-SHA-2-(hmac-sha2-256, hmac-sha2-512) and GCM (AEAD_AES_-256_GCM)	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support), [RFC6668], [RFC5647] (GCM for SSH)	256, 512	Yes	
7	Key generation for host and user keys	RSA key generation with key size: 3072, 4096 bits	[FIPS 186-5], B.3.1 and C.1 for Miller Rabin primality tests.	3072, 4096	Yes	
8	Key generation for host and user keys	ECDSA key generation based on NIST curves: P-384 and P-521	[FIPS 186-5],A.2	384, 521	Yes	
9	Key generation for diffie-hellman key agreement	Modular exponentiation DH key exchange with key size: 3072, 4096	[SP800-56A-Rev3] sec. 5.6.1.1.4	4096, 8192 (prime modulus)	Yes	
10	Key generation for diffie-hellman key exchange	ECDH key generation based on the NIST curves: P-384 and P-521	[SP800-56A-Rev3], sec. 5.6.1.2.2	384, 521	Yes	
11	Trusted channel	FTP_ITC_EXT.1, [ST] sec. 7.2.8.1 for SSH v2	Cf. all lines above	See above	Yes	

Table 3: TOE cryptographic functionality for SSH

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Key derivation with authentication (access control, protection / recovery mode)	Password based key derivation using PBKDF2 with PRF HMAC using SHA-256, SHA-384, SHA-512	[SP800-132] [RFC2898] (PBKDF2) [FIPS198-1] (HMAC), [FIPS180-4] (SHA)	Guessing prob. 2^{-20} Salt 32 byte (LUKS_SALTSIZE) iteration count 2000 ms	Yes	
2	Confidentiality (bulk data & key access / key wrapping)	AES in XTS mode IV-handling mechanism: XTS-plain64 XTS-benbi	[FIPS197] [SP800-38E] (XTS)	2*256	Yes	

Table 4: TOE cryptographic functionality for dm-crypt

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Confidentiality	Cipher: AES Modes: CBC, GCM	CBC: [RFC5246], [SP800-38A] GCM: [RFC5288], [SP800-38D]	256	Yes	
2	Integrity and authenticity	HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 AES GMAC used by GCM	[RFC5246] [RFC5288] [FIPS180-4] (SHA) [FIPS198-1] (HMAC) [SP800-38D] (GCM / GMAC)	256, 384, 512	Yes	
3	IV / Key derivation	PRF SHA-2 with hash type chosen by TLS cipher suite	[RFC5246] [FIPS180-4] [FIPS198-1]	256	Yes	
4	Peer authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-2	[RFC5246] [FIPS186-5] [FIPS180-4] [RFC8017] (PKCS#1 v2.2) Sec. 8 (RSA)	3072, 4096	Yes	
5	Peer	RSA signature	[RFC8446]	3072, 4096	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
	authentication	generation and verification RSASSA-PSS using SHA-2	[FIPS186-5] [FIPS180-4] [RFC8017] (PKCS#1 v2.2) Sec. 8 (RSA)			
6	Peer authentication	ECDSA with signature generation and verification using SHA-2 with NIST P-384, P-521	[RFC5289] Sec1-v2 (ECDSA) ([SEC2]) [FIPS180-4] (SHA)	384, 521	Yes	
7	Key generation for authentication	ECDSA using NIST P-384, P-521	[FIPS186-5] A.2	256, 384	Yes	
8	Key generation for authentication	RSA with 3072, 4096 bits	[FIPS186-5] B.3.1 and C.1 for Miller primality tests	3072, 4096	Yes	
9	Key generation for DH / ECDH	FFC key-pair generation using PQG parameter set	[SP800-56A-Rev3] section 5.6.1.1.4	3072, 4096	Yes	
10	Key generation for DH / ECDH	ECC key-pair generation with NIST P-384, P-521	[SP800-56A-Rev3] section 5.6.1.2.2	384, 521	Yes	
11	Trusted channel	FTP_ITC_EXT.1, ST [5] sec. 7.2.8.1 for TLS v1.2	Cf. all lines for TLS above	See above	Yes	
12	Random number generator	CTR DRBG with AES- 256, with DF, without PR	[SP800-90A-Rev1]	n/a	n/a	

Table 5: TOE cryptographic functionality for TLS

References for tables 3 to 5:

ANSIX9.62 **Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA)**
Date 2005-11-16
Location https://standards.globalspec.com/std/1955141/ANSI%20X9.62

FIPS180-4 **Secure Hash Standard (SHS)**
Date 2015-08-04
Location https://csrc.nist.gov/pubs/fips/180-4/upd1/final

FIPS186-5 **Digital Signature Standard (DSS)**
Date 2023-02-03
Location https://csrc.nist.gov/pubs/fips/186-5/final

FIPS197 **Advanced Encryption Standard (AES)**
Date 2023-05-09
Location https://csrc.nist.gov/pubs/fips/197/final

FIPS198-1 **The Keyed-Hash Message Authentication Code (HMAC)**
Date 2008-07-16
Location https://csrc.nist.gov/pubs/fips/198-1/final

RFC2104 **HMAC: Keyed-Hashing for Message Authentication**
Author(s) H. Krawczyk, M. Bellare, R. Canetti
Date 1997-02-01
Location http://www.ietf.org/rfc/rfc2104.txt

RFC2898 **PKCS #5: Password-Based Cryptography Specification Version 2.0**
Author(s) B. Kaliski
Date 2000-09-01

RFC4251 **The Secure Shell (SSH) Protocol Architecture**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4251.txt

RFC4252 **The Secure Shell (SSH) Authentication Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4252.txt

RFC4253 **The Secure Shell (SSH) Transport Layer Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4253.txt

RFC4419 **Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol**
Author(s) M. Friedl, N. Provos, W. Simpson
Date 2006-03-01
Location http://www.ietf.org/rfc/rfc4419.txt

RFC5246 **The Transport Layer Security (TLS) Protocol Version 1.2**
Author(s) T. Dierks, E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5246.txt

RFC5288 **AES Galois Counter Mode (GCM) Cipher Suites for TLS**
Author(s) J. Salowey, A. Choudhury, D. McGrew
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5288.txt

RFC5289 **TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)**
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5289.txt

RFC5647 **AES Galois Counter Mode for the Secure Shell Transport Layer Protocol**
Author(s) K. Igoe, J. Solinas
Date 2009-08-01
Location http://www.ietf.org/rfc/rfc5647.txt

RFC5656 **Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer**
Author(s) D. Stebila, J. Green
Date 2009-12-01
Location http://www.ietf.org/rfc/rfc5656.txt

RFC5903 **Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2**
Author(s) D. Fu, J. Solinas
Date 2010-06-01
Location http://www.ietf.org/rfc/rfc5903.txt

RFC6668 **SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol**
Author(s) D. Bider, M. Baushke

	Date 2012-07-01 Location http://www.ietf.org/rfc/rfc6668.txt
RFC8017	**PKCS #1: RSA Cryptography Specifications Version 2.2** Author(s) B. Kaliski, J. Jonsson, A. Rusch Date 2016-11-01 Location http://www.ietf.org/rfc/rfc8017.txt
RFC8268	**More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)** Author(s) M. Baushke Date 2017-12-01 Location http://www.ietf.org/rfc/rfc8268.txt
RFC8332	**Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol** Author(s) D. Bider Date 2018-03-01 Location http://www.ietf.org/rfc/rfc8332.txt
RFC8446[8]	**The Transport Layer Security (TLS) Protocol Version 1.3** Author(s) E. Rescorla Date 2018-08-01 Location http://www.ietf.org/rfc/rfc8446.txt
SEC2	**Recommended Elliptic Curve Domain Parameters** Date 2000 Location http://www.secg.org
SP800-132	**Recommendation for Password-Based Key Derivation: Part 1: Storage Applications** Date 2010-12-22 Location https://csrc.nist.gov/pubs/sp/800/132/final
SP800-186	**Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters** Date 2023-02-03 Location https://csrc.nist.gov/pubs/sp/800/186/final
SP800-38A	**Recommendation for Block Cipher Modes of Operation: Methods and Technique** Date 2001-12-01 Location https://csrc.nist.gov/pubs/sp/800/38/a/final
SP800-38D	**Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** Date 2007-11-28 Location https://csrc.nist.gov/pubs/sp/800/38/d/final
SP800-38E	**Recommendation for Block Cipher Modes of Operation: the XTSAES Mode for Confidentiality on Storage Devices** Date 2010-01-18 Location https://csrc.nist.gov/pubs/sp/800/38/e/final
SP800-56A-Rev3	**Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography** Date 2018-04-16 Location https://csrc.nist.gov/pubs/sp/800/56/a/r3/final
SP800-90A-Rev1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** Date 2015-06-24 Location https://csrc.nist.gov/pubs/sp/800/90/a/r1/final

[8] RFC 8446 for TLS 1.3 also specifies new requirements for TLS 1.2 implementations

Note: End of report