Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1248-2026

for

SUSE Linux Enterprise Server 15 SP4

from

SUSE Software Solutions Germany 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-1248-2026 (*)

Operating Systems

SUSE Linux Enterprise Server 15, SP4

from	SUSE Software Solutions Germany GmbH
PP Conformance:	Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010, OSPP Extended Package – Advanced Audit, Version 2.0, 28 May 2010, OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
valid until:	23 February 2031

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

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

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 under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

[4] Proclamation of the 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 SUSE Linux Enterprise Server 15, SP4 has undergone the certification procedure at BSI.

The evaluation of the product SUSE Linux Enterprise Server 15, SP4 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 applicant is: SUSE Software Solutions Germany GmbH.

The product was developed by: SUSE Software Solutions Germany GmbH.

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

5. Validity of the Certification Result

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

- all stipulations regarding generation, configuration and operation, as given in the evaluated guidance documentation, 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:

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 SUSE Linux Enterprise Server 15, SP4 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 Software Solutions Germany GmbH
Frankenstraße 146
90461 Nürnberg
Germany

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, a highly-configurable Linux-based operating system which 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 Protection Profile Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010,
OSPP Extended Package – Advanced Audit, Version 2.0, 28 May 2010,
OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.2. 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 Linux kernel implements the core of the LAF functionality. It gathers all audit events, analyses these events based on the audit rules and forwards the audit events that are requested to be audited to the audit daemon executing in user space. Audit events are generated in various places of the kernel. In addition, a user space application can create audit records which needs to be fed to the kernel for further processing.
Cryptographic services	The TOE provides cryptographically secured network communication channels to allow remote users to interact with the TOE. Using one of the following cryptographically secured network channels, a user can request the following services: • OpenSSH: The OpenSSH application provides access to the command line interface of the TOE. Users may employ OpenSSH for interactive sessions as well as for non-interactive sessions. The console provided via OpenSSH provides the same environment as a local console. OpenSSH implements the SSHv2 protocol. • libvirtd: The libvirtd daemon is the management facility to allow remote users to configure virtual machines. The configuration covers all aspects such as assigning of resources, starting or stopping of virtual machines. libvirtd directly interacts with the virtual machines. This interface is protected using OpenSSH. • VNC: The VNC interface provides the access mechanism for users to interact with the console of a virtual machine. The VNC connection is tunneled through OpenSSH. • IPSec: The strongSwan application suite implements the IKEv1 and IKEv2 protocol family to negotiate the ISAKMP SA as well as the IPSec SA to securely establish session keys used for the IPSec network protocol. The established session keys are transferred to the kernel which implements the generation as well as processing of ESP and AH packets as part of the IPSec operation. Note, the evaluation only covers the IKEv2 protocol. In addition to the cryptographically secured communication channels, the TOE also

TOE Security Functionality	Addressed issue
	provides cryptographic algorithms for general use. The cryptographic primitives for implementing the above mentioned cryptographic communication protocols are provided by OpenSSL.
Packet Filter	The packet filter functionality allows network packet filtering on the link layer (ebtables) and higher network layers (iptables). • iptables: provides stateful and stateless packet filtering for network communication by inspecting the IP header, the TCP header, UDP header and/or ICMP header of every network packet that passes the network stack.
Identification and Authentication	User identification and authentication in the TOE includes all forms of interactive login (e.g. using the SSH protocol or log in at the local console) as well as identity changes through the su and sudo commands. These all rely on explicit authentication information provided interactively by a user. In addition, the key-based authentication mechanism of the OpenSSH server is another form of of authentication. Linux uses a suite of libraries called the "Pluggable Authentication Modules" (PAM) that allow an administrative user to choose how PAM-aware applications authenticate users. The TOE provides PAM modules that implement all the security functionality to: • Provides login control and establishing all UIDs, GIDs and login ID for a subject • Ensure the quality of passwords • Enforce limits for accounts (such as the number of maximum concurrent sessions allowed for a user) • Enforce the change of passwords after a configured time including the password quality enforcement • Enforcement of locking of accounts after failed login attempts. • Restriction of the use of the root account to certain terminals • Restriction of the use of the su and sudo commands In addition to the PAM-based authentication outlined above, the OpenSSH server is able to perform a key-based authentication. When a user wants to log on, instead of providing a password, the user applies his SSH key. After a successful verification, the OpenSSH server considers the user as authenticated and performs the PAM-based operations as outlined above. The TOE uses the screen(1) application which locks the current session of the user either after an administrator-specified time of inactivity or upon the user's request. To unlock the session, the user must supply his password. Screen uses PAM to validate the password and allows the user to access his session after a successful validation.
Discretionary Access Control	DAC provides the mechanism that allows users to specify and control access to objects that they own. DAC attributes are assigned to objects at creation time and remain in effect until the object is destroyed or the object attributes are changed. DAC attributes exist for, and are particular to, each type of named object known to the TOE. DAC is implemented with permission bits and, when specified, ACLs. The TOE supports standard UNIX permission bits to provide one form of DAC for file system objects in all supported file systems. There are three sets of three bits that define access for three categories of users: the owning user, users in the owning group, and other users. The three bits in each set indicate the access permissions granted to each user category: one bit for read (r), one for write (w) and one for execute (x). Note that write access to file systems mounted as read only (e. g. CD-ROM) is always rejected (the exceptions are character and block device files which can still be written to as write operations do not modify the information on the storage media). The SVTX (sticky) attribute is used for world-writeable temp directories preventing the removal of files by users other than the owner. The TOE provides support for POSIX type ACLs to define a fine grained access control on a user basis. An ACL entry contains the following information: A tag type that

TOE Security Functionality	Addressed issue
	specifies the type of the ACL entry, a qualifier that specifies an instance of an ACL entry type, and a permission set that specifies the discretionary access rights for processes identified by the tag type and qualifier.
Authoritative Access Control	The TOE supports a type of access control which is based on labels assigned to objects of subjects that only authorized administrators can set and modify. The TOE implements the following types of access control restrictions to limit virtual machines to access only their resources: • AppArmor-based: each virtual machine and its resource is assigned to a unique AppArmor label which prevents other virtual machines with different labels to access either the virtual machine process or its resources. • Cgroup-based: each virtual machine is granted access to a white list of device files. Access to other device files is prevented using the cgroup device ACL mechanism.
Virtual Machine Environments	KVM is implemented as part of the Linux kernel supported by user space code. It consists of two essential components that implement VMM functionality: the KVM Linux kernel module and QEMU for hardware emulation. The use of QEMU implies that KVM provides full virtualization to its guests and can, therefore, execute unaltered guest operating systems. The KVM Linux kernel module implements memory management and virtual machine maintenance functionality. This kernel extension makes the entire Linux kernel the hypervisor. Virtual machines are treated by the Linux kernel as normal applications. The kernel schedules them like applications, and they can be handled like applications. As such, the process implementing a virtual machine can be seen in process listings and it can be sent regular signals, like SIGTERM. From the Linux kernel perspective, the virtual machine is just another process. However, the virtual machine process has a special layout. The process image is split into two parts. The first part hosts a regular application logic executing in user mode – this is used to maintain the QEMU I/O virtualization and some other small KVM-related software components. The second part contains the image of the guest code, usually an operating system, where the software may execute either in supervisor or user mode of the processor. This implies that the entire memory used for the guest operating system is allocated by the QEMU application. The kernel keeps track of which parts of the application belong to the guest operating system and which parts to the regular application.
Security Management	The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of TSF. The configuration of TSF are hosted in the following locations: • Configuration files (or TSF databases) • Data structures maintained by the kernel and within the kernel memory The TOE provides applications to authorized users as well as authorized administrators to perform various administrative tasks. These applications are documented as part of the administrator and user guidance. These applications are either used to modify configuration files or to access parameters controlled and enforced by the kernel via kernel-provided interfaces to user space. Using the sudo command, authorized administrators can approve that other users can perform management tasks. Once the administrator approves the operation, the /etc/sudoers file is modified to grant the user the right to perform the administrative operation.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [5], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [5], chapter 3.1.1, 3.2 and 3.3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 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 15, SP4

The following table outlines the TOE deliverables (all Hash sums SHA256):

No	Type	Identifier	Release	Form of Delivery
1	ISO	SLE-15-SP4-Full-x86_64-QU4-Media1.iso (56e6a86ccbd47c989f6ef41714d764d0a2d15a6e49b2dbfd618fa42640877f17)	SLES 15 SP4	D/L
2	ISO	SLE-15-SP4-Full-aarch64-QU4-Media1.iso (aed86f7a3446761b719640090b62e1013e9a65972e5fdaaa4fb653dc3a311afa)	SLES 15 SP4	D/L
3	ISO	SLE-15-SP4-Full-s390x-QU4-Media1.iso (63bcc73011e53a8912a8e0cacdc3c3991fb34af8c4b94a3a08d32cf2e85e5977)	SLES 15 SP4	S/L
4	DOC	Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server Version 15 SP4 [9] (63b88e3641972bc0c2bdd3cecac46be661c02bb6f253b3220e297aad0607e2c5)	V1.0	D/L
5	rpm*	kernel	default-5.14.21-150400.24.184.1	D/L and verification through TOE
6	rpm*	openssh openssh-server openssh-clients openssh-helpers openssh-common	8.4p1-150300.3.57.1	D/L and verification through TOE
7	rpm*	libssh4	0.9.8-150400.3.9.1	D/L and verification through TOE
8	rpm*	systemd	249.17-150400.8.49.2	D/L and verification through TOE

No	Type	Identifier	Release	Form of Delivery
9	rpm*	polkit	0.116-150200.3.15.1	D/L and verification through TOE
10	rpm*	sudo	1.9.9-150400.4.39.1	D/L and verification through TOE
11	rpm*	libxml2	2-2.9.14-150400.5.44.1	D/L and verification through TOE
12	rpm*	pam	1.3.0-150000.6.83.1	D/L and verification through TOE
13	rpm*	pam_pkcs11	0.6.10-150100.3.11.1	D/L and verification through TOE
14	rpm*	pam-config	1.1-150200.3.14.1	D/L and verification through TOE
15	rpm*	libblockdev	2.26-150400.3.5.1	D/L and verification through TOE
16	rpm*	openssl	1_1-1.1.1l-150400.7.78.1	D/L and verification through TOE
17	rpm	audit-audispd-plugins	3.0.6-150400.4.16.1	D/L and verification through TOE
18	rpm	nftables	0.9.8-150300.3.6.1	D/L and verification through TOE
19	rpm	firewalld	0.9.3-150400.8.12.1	D/L and verification through TOE

Table 2: Deliverables of the TOE

The delivery of the TOE is electronic download only in the form of network or USB ISO images according to [9]. The TOE parts that must or may be downloaded and installed after installation of the ISO are shown in Scope of TOE Supply (section 2). Those parts that MUST be downloaded and installed are marked with an "*" following the "rpm" in column "type".

The packages that make up the TOE are digitally signed using GPG. The key of the developer is contained on the installation ISO, as described in [9]. This key is also used to verify the necessary additional packages mentioned in the [9].

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. The [9] is a central document to the evaluation. It defines how to install and configure the TOE.

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: Auditing, Cryptographic support, Packet filter, Identification and Authentication, Discretionary Access Control, Authoritative Access Control, Virtual machine environments and Security Management.

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:

- Those responsible for the TOE are competent and trustworthy
- If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected.
- Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. (e.g. network cabling, DAC protections on security-relevant files, etc.).
- Those responsible for the TOE must ensure that the system is installed and configured in a secure manner.
- Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
- Those responsible for the TOE must ensure that the TOE is protected from physical attacks.
- Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
- Those responsible for the TOE must ensure that remote trusted IT systems are protected equivalently to the TOE.
- The trusted IT systems executing the TOE support the enforcement of the security policy.

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

5. Architectural Information

The TOE is structured in much the same way as many other operating systems, especially Unix-type operating systems. It consists of a kernel, which runs in the privileged state of the processor and provides services to applications (which can be used by calling kernel services via the system call interface). Direct access to the hardware is restricted to the kernel, so whenever an application wants to access hardware like disk drives, network interfaces or other peripheral devices, it has to call kernel services. The kernel then checks if the application has the required access rights and privileges and either performs the service or rejects the request.

The kernel is also responsible for separating the different user processes. This is done by the management of the virtual and real memory of the TOE which ensures that processes executing with different attributes cannot directly access memory areas of other processes but have to do so using the inter-process communication mechanism provided by the kernel as part of its system call interface.

The TSF of the TOE also include a set of trusted processes, which when initiated by a user, operate with extended privileges. The programs that represent those trusted

processes on the file system are protected by the file system discretionary access control security function enforced by the kernel.

In addition, the execution of the TOE is controlled by a set of configuration files, which are also called the TSF database. Those configuration files are also protected by the file system discretionary access control security function enforced by the kernel.

The kernel acts as a hypervisor for the virtual machine support of the TOE. It uses the virtualization support of the underlying processor to provide virtual machines with the required kernel support in KVM and user space support via libvirt.

Normal users – after they have been successfully authenticated by a defined trusted process – can start untrusted applications where the kernel enforces the security policy of the TOE when those applications request services from the kernel via the system call interface.

The TOE includes a secure system initialization function which brings the TOE into a secure state after it is powered on or after a reset. This function ensures that user interaction with the TOE can only occur after the TOE is securely initialized and in a secure state.

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 evaluated configuration is presented in the ECG [9] and the ST [5]. It defines a number of hardware platforms in the ECG [9] section 1.3.1 as well as in the ST [5], section 1.4.4:

- x86 64bit Intel processors, with Cascade Lake Microarchitecture
- x86 64bit AMD processors, with ZEN 3 Microarchitecture
- ARM processors, with ARMv8.2-A Microarchitecture
- IBM z15 with TOE executing within an LPAR

The installation of the TOE must be carried out as described in the ECG [9], which describes the actual installation steps and additional configuration steps that need to be carried out when the TOE is installed.

7.1. Developer Testing approach

The test plan provided by the developer lists test cases by groups, which reflects the mix of sources for the test cases. The provided mapping lists the SFRs and the TSFI the test cases are associated with. The test plan is focused on the security functions of the TOE and ignores other aspects typically found in developer test plans. The test cases are mapped to the corresponding functional specification and the subsystems described in Part II and III of the high level description [10].

The developer uses two test suites (audit-test and LTP) as bases for the testing and adapted them as needed. The test suites have a longer history for linux testing in general (their based versions are also available online). Specifically for the audit-test suite, it is designed with an installed SELinux LSM in mind. The developer adapted the test suite to either only cover the tests that were deemed relevant per coverage analysis or ignored and justified remaining test failures not fitting the SUSE OS setup. The developer executed a number of further smaller test sets in the area of KVM, authentication auditing, IPSEC, and apparmor which partly also make use of the audit-test framework.

The test suites has a common framework for the automated tests in which individual test cases adhere to a common structure for setup, execution and cleanup of tests. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behavior with illegal parameters and reaction to missing privileges). Each test within a test case reports PASS, OK or FAIL and the test case summary in batch mode reports PASS if all the tests within the test case passed, otherwise FAIL.

The developer decided to only perform a subset of tests against the final TOE which is a bugfix update of the kernel and the OpenSSH packages considering that the subset focusses on the kernel and also covers SSH functionality.

Testing results

The test results are provided by the developer in form of log files for all supported hardware platforms. As described in the testing approach, the test results of all the automated tests are written to files. The results of the manual tests have also been documented in a separate file.

All test results from all tested environments show that the expected test results are identical to the actual test results.

Test coverage

The test mapping provided by the developer shows that the tests cover all individual TSFI identified for the TOE.

Test depth

In addition to the mapping to the functional specification, the developer provided a mapping of test cases to subsystems of the high-level design and the internal interfaces described therein. This mapping shows that all subsystems and the internal interfaces are covered by test cases. To show evidence that the internal interfaces have been called, the developer provided the description of the internal interfaces as part of the high-level design. The interfaces are well defined, to allow the evaluator to assess whether they have been covered by testing. Not all of the internal interfaces mentioned in the high-level design could be covered by direct test cases. Some internal interfaces can – due to the restrictions of the evaluated configuration – only be invoked during system startup. This includes especially internal interfaces to load and unload kernel modules, to register / de-register device drivers and install / de-install interrupt handlers. Since the evaluated configuration does not allow to dynamically load and unload device drivers as kernel modules, those interfaces are only used during system startup and are, therefore, implicitly tested there.

Conclusion

The evaluator has verified that developer testing was performed on hardware conform to the ST. The evaluator was able to follow and fully understand the developer testing approach by using the provided test documentation.

The evaluator analyzed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem/internal interfaces identified in appendix B of High-level design [10].

The evaluator reviewed the test results provided by the developer and found them to be consistent with the expected test results according to the test plan.

7.2. Evaluator Testing Effort

The evaluator performed the automated audit-test suite of the developer and a number of additional tests. The evaluator tested on all supported TOE platforms. A rough break down (differs slightly between the platforms) of the test numbers:

- audit-test: 338
- IPSec/SSH: 16
- pam: 9
- miscellaneous: 5

Test approach and depth

In addition to the developer tests, the evaluator devised tests for a subset of the TOE functionality as follows:

- increasing the cryptographic algorithm coverage for IPsec, SSH, and dm-crypt
- additional tests to show weak algorithms get rejected
- increasing coverage of FIA_AFL.1 and FIA_UAU.7 (failed authentication lockout and password obstruction) that apply to a range of interfaces and commands
- tests for simple but potentially security-relevant command not covered by developer tests (newgrp, star, create_module)
- rerun of the Linux RNG entropy test as done in the BSI study with focus on the IRQ entropy source

The evaluator tested all security functions, with increased variations for some interface and used cryptographic algorithms.

TOE test configuration

The used test systems had the TOE version SLES 15 SP4 installed. The evaluator verified the test systems according to the documentation in the Evaluated Configuration Guide [9] and the test plan. As assessed in the evaluation report on the administrator guidance, the ECG [9] is consistent with the ST [5]. Hence, the evaluator concludes that the evaluator's configuration is consistent with the ST.

The evaluator performed tests on all hardware architectures types supported in the evaluation.

Test results

The testing was successful.

7.3. Evaluator Penetration Testing

The evaluator performed 10 test cases. Linux standard tools (strace, GNU C compiler, nmap) have been used as part of the testing.

Test approach and Depth

The evaluator used the MITRE CVE portal, SUSE support center, and Google searches for finding publicly documented vulnerabilities. That lead to some tests in the areas of CPU checks.

Another area were systematic DBus function privilege tests against the DBus interfaces and their registered services.

Several of the evaluator tests were not penetration tests in terms of trying to break a functionality, but to determine the available attack surface in various contexts: configuration files, setuid programs, netlink subprotocol accessibility.

One particular test attempts to trigger a operational failure due to invalid netlink messages and fuzzing the hypervisor through variations of VM guest code. In summary, the following aspects were subject to testing:

1. Undocumented security-relevant programs
2. Potentially inappropriate access control to configuration files
3. Unmitigated OS-relevant CPU vulnerabilities
4. Potentially inappropriately controlled DBus services
5. Potentially insecure netlink message processing
6. Potential additional netlink interfaces into the kernel
7. Incomplete failed authentication lockout handling
8. KVM op code fuzzing
9. CPU vulnerability PoC check (CVE-2024-28956)

In addition an pattern search in reported vulnerabilities with regard to affected components and impact scoring has been performed.

Configuration

The TOE was in its evaluated configuration as described in the Evaluated Configuration Guide [9]. All supported platforms (Intel, AMD, ARM, s390) have been involved in the penetration testing. Some tests were not executed on all platforms, e.g., the KVM tests were tailored to the Intel platform. The documentation of the individual tests identified the specific platform used by the test.

Results

No deviation from the expected results have been found.

8. Evaluated Configuration

This certification covers the following configurations of the TOE, listed in the Evaluated Configuration Guide (ECG) [9] section 1.3.1 as well as in ST [6], section 1.4.4:

- x86 64bit Intel processors, with Cascade Lake Microarchitecture
- x86 64bit AMD processors, with ZEN 3 Microarchitecture
- ARM processors, with ARMv8.2-A Microarchitecture
- IBM z15 with TOE executing within an LPAR

The installation of the TOE must be carried out as described in the ECG [9], which describes the actual installation steps as well as additional configuration steps that need to be carried out when the TOE is installed.

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used. For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The component ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
  OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010,
  OSPP Extended Package – Advanced Audit, Version 2.0, 28 May 2010,
  OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010 [7]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3

The TOE mainly consists of open source software. It is common to share flaw information in its community.

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 table in annex C 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. 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. Definitions

12.1. Acronyms

AH Authentication Header

AIS Application Notes and Interpretations of the Scheme

ACL Access Control List

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

CVE Common Vulnerabilities and Exposures

DAC Discretionary Access Control

EAL	Evaluation Assurance Level
ECG	Evaluated Configuration Guide
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KVM	Kernel Virtualized Machine
LAF	Lightweight Audit Framework
LSM	Linux Security Module
LUKS	Linux Unified Key Setup
PP	Protection Profile
QEMU	Quick Emulator
RNG	Random Number Generator
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network

12.2. Glossary

AppArmor - A Linux kernel security module (LSM) that is able to implement arbitrary security policies. An AppArmor policy distributed with the TOE implements multi-level or multi-category security.

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.

DAC - Discretionary Access Control implemented with permission bits and ACLs.

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

PAM - Pluggable Authentication Module - the authentication functionality provided with Linux is highly configurable by selecting and combining different modules implementing different aspects of the authentication process.

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.

SELinux - see AppArmor.

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.

13. 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

[5] Security Target for SUSE Linux Enterprise Server 15 SP4 including KVM Virtualization BSI-DSZ-CC-1248-2026, Version 4.0, 2026-02-20, SUSE Software Solutions Germany GmbH

[6] Final Evaluation Technical Report, Version 3, 2026-02-20, atsec information security GmbH (confidential document)

[7] Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010,
OSPP Extended Package – Advanced Audit, Version 2.0, 28 May 2010,
OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010

[8] MASTER CM List, 2026-02-20, SUSE Software Solutions Germany GmbH (confidential document)

[9] Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP4, Version 1.0, 2026-02-19, SUSE Software Solutions Germany GmbH

[10] Linux Specification High-level design, 2024-10-24, SUSE Software Solutions Germany GmbH (confidential document)

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler (Collection of Developer Evidence)
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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-1248-2026

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
0	Authentication	The client authenticates either with UserID & password or by cryptographic means as shown in #1 and #2 and verified by the server, respectively				
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 (SSHAUTH) for user authentication [RFC8332] for rsa-sha2-256/512	3072, 4096	Yes	Pubkeys are exchanged trustworthily out of band, e.g. checking fingerprints. Authenticity is not part of the TOE. (no certificates are used)
2	Authentication	ECDSA signature generation and verification using P-256/384/521 (ecdsa-sha2-nistp256, ecdsa- sha2-nistp384, ecdsa-sha2-nistp521)	[ANSIX9.62] (ECDSA), [FIPS180-4] (SHA), NIST curves [SP800-186] identifiers for P-256/384/521 [RFC5656] [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	256, 384, 521	Yes	
3	Key Agreement	ECDH with P-256/384/521 (ecdh-sha2-nistp256, ecdhsha2-nistp384, ecdh-sha2-nistp521)	[RFC4253] (SSH-TRANS) [FIPS-180-4] (SHA) supported by [RFC5656] (ECC in SSH) P-256/384/521 NIST curves [SP800-186]	256, 384, 521	Yes	
4	Confidentiality	AES in CTR and GCM mode (aes128-ctr,	[FIPS197] (AES), [RFC 4344]	128, 256	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
		aes192-ctr, aes256-ctr) (aes128-gcm@openssh.com, aes256-gcm-@openssh.com)	(SSH-TRANS using AES with CTR mode), [RFC5647] (SSH-2 using AES with GCM mode)			
5	Integrity and Authenticity	HMAC-SHA-2-(hmacsha2-256, hmacsha2-512, hmacsha2-256-etm@openssh.com, hmac-sha2-512-tm@openssh.com) and GCM (AEAD_AES_-128_GCM, AEAD_AES_-256_GCM)	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support), [RFC6668], [RFC5647]	256, 512	Yes	etm = encryptthen MAC(Open SSH 8.4)
6	Key generation for host and user keys	RSA key generation with key size: 3072, 4096 bits	[FIPS 186-5], B.3.1 and C for Miller Rabin primality tests.	3072, 4096	Yes	
7	Key generation for host and user keys	ECDSA key generation based on NIST curves: P-256, P-384, and P-521	[FIPS 186-5], A.2	256, 384, 521	Yes	
8	Key generation for diffie-hellman key exchange	ECDH key generation based on the NIST curves: P-256, P-384, and P-521	[SP800-56ARev3] , sec. 5.6.1.2.2	256, 384, 521	Yes	
9	Trusted channel	FTP_ITC_EXT.1, [5] sec. 7.1.2.1 for SSH v2	Cf. all lines above	See above	Yes	

Table 3: TOE cryptographic functionality SSH

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	IKE authenticatio n	RSA signature generation and verification RSASSA-PSS using SHA-256 and SHA-384 (Auth Method 14)	[RFC7296] (IKEv2) [RFC3447] (RSA) [FIPS180-4] (SHA) [RFC7427] (IKEv2 RSASSAPSS)	3072, 4096	Yes	
2	IKE authenticatio n	ECDSA signature generation and verification with	[FIPS 186-5] [FIPS180-4] (SHA)	256, 384, 521	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
		SHA-256 on P-256 curveSHA-384 on P-384 curve SHA-521 on P-521 curve (Auth Method 9, 10, 11)	[RFC4754] (IKEv2 using ECDSA), EC secp{256, 384, 521}r1 [SEC2]			
3	IKE key agreement	DH with MODP groups: exponentiation groups modulo a prime	[RFC7296] (IKEv2), [DH] (DH as referenced in [RFC7296]) [RFC3526] groups 15, 16, 17,18 (3072, 4096, 6144, 8192)-bit MODP groups	3072, 4096, 6144, 8192	Yes	
4	IKE key derivation	PRF based on: HMAC with SHA-256(ID 5 PRF_HMAC_SHA2_ 256) HMAC with SHA-384(ID 6 PRF_HMAC_SHA2_384) HMAC with SHA-512(ID 7 PRF_HMAC_SHA2_512)	[RFC7296] (IKEv2), [FIPS198-1] (HMAC), [FIPS180-4] (SHA) [RFC4868] (HMAC -SHA2 with IPsec) [IKEV2IANA]	|k| = variable[8]	Yes	IKE keys (IKE SA) and Ipsec keys (Ipsec SA / child SA) are derived according to required for the negotiated algorithms they are used for[9]
5	IKE integrity and authenticity and IPsec ESP integrity and authenticity	HMAC with SHA-256-12-8(ID 12 AUTH_HMAC_-SHA2_256_128) HMAC with SHA-384-19-2(ID 13 AUTH_HMAC_-SHA2_384_192) HMAC with SHA-512-25-6(ID 14 AUTH_HMAC_-SHA2_512_256)	[RFC4868]. (HMAC-SHA2 with IPsec)	256, 384, 512	Yes	
6	IKE encryption and IPsec ESP encryption	AES in CBC mode(ID 12 ENCR_AES_CBC)	[RFC7296], [RFC3602]	128, 192, 256	Yes	
7	IKE	AES in CTR mode	[RFC5930]	128, 192,	Yes	

[8]referred key size = size of the output of the underlying hash function / key size of AES = 128 bit

[9]Note that for IKEv2 the whole PRF is negotiated not as within IKEv1 where the hash is negotiated separately.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
	encryption and IPsec ESP encryption	(ID 13 ENCR_AES_CTR)	(AES-CTR for IKEv2) [RFC3686] (AES-CTR for ESP)	256		
8	IKE authenticated encryption and IPsec ESP authenticated encryption	AES in CCM mode(ID 15 ENCR_AES-CCM_12) (ID 16 ENCR_AES-CCM_16)	[RFC5282], [RFC4309], [RFC5116]	128, 192, 256	Yes	
9	IKE authenticated encryption and IPsec ESP authenticated encryption	AES in GCM mode (ID 19 AES-GCM with a 12 octet ICV) (ID 20 AES-GCM with a 16 octet ICV)	[RFC5282], [RFC4106], [RFC5116]	128, 192, 256	Yes	
10	Key generation	RSA key generation with key size: 3072, 4096 bits	[FIPS 186-5], A.1.3 and C.3 and B.3 for Miller Rabin primality tests.	n/a	n/a	Keys for certificates and for certificate signing Using either FCS_RNG.1 (SSL)
11	Key generation	ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS 186-5], A.4	n/a	n/a	
12	Trusted Channel	FTP_ITC.1 b), [ST] sec. 7.1.2.2 for IKEv2, Ipsec ESP	Cf. all lines above, especially [RFC7296] (IKEv2) [RFC4303] (ESP)	See above	Yes	Either in transport mode or in tunnel mode

Table 4: TOE cryptographic functionality IPsec

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
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] [CFLUKS]4 [RFC2898] (PBKDF2) [FIPS198-1] (HMAC), [FIPS180-4] (SHA)	Guessing prob. 2^{-20} Salt 32 byte (LUKS_SALTSIZE)	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*128, 2*192, 2*256	Yes

Table 5: TOE cryptographic functionality dm-crypt

Note: End of report