Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1151-2021

for

SUSE Linux Enterprise Server Version 15 SP2

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-1151-2021 (*)

Betriebssysteme

SUSE Linux Enterprise Server, Version 15 SP2

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 – Advanced Management, Version 2.0, 28 May 2010, OSPP Extended Package – Advanced Audit, Version 2.0, 28 May 2010, OSPP Extended Package – Virtualization, 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

SOGIS
Recognition Agreement

Common Criteria

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

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

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

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

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

Bonn, 8 July 2021

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product SUSE Linux Enterprise Server, Version 15 SP2 has undergone the certification procedure at BSI.

The evaluation of the product SUSE Linux Enterprise Server, Version 15 SP2 was conducted by atsec information security GmbH. The evaluation was completed on 2 July 2021. 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 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 following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 July 2021 is valid until 7 July 2026. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

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

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product SUSE Linux Enterprise Server, Version 15 SP2 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] SUSE Software Solutions Germany GmbH
Maxfeldstr. 5
90409 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 [6] 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 and three OSPP Extended Packages [8]:

- Advanced Management, Version 2.0, 28 May 2010,
- Advanced Audit, Version 2.0, 28 May 2010 and
- Virtualization, Version 2.0, 28 May 2010

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 [6], 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

TOE Security Functionality	Addressed issue
	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 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. ● ebtables: Similarly to the netfilter, ebtables implements chains that are used by ebtables to apply filtering. It provides filtering based on protocol information frame addresses
Indentification 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

TOE Security Functionality	Addressed issue
	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 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 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

TOE Security Functionality	Addressed issue
	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 [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], 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 [6], chapters 3.1.3, 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 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

SUSE Linux Enterprise Server, Version 15 SP2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW / ISO Image	SLE-15-SP2-Full-x86_64-QU1-Media1.iso (SHA256: 64aea562b5f51381b57f0c295fdd96c49b64c5f0760f2b62752fca54f4d999fd)	SLES 15 SP2	Download
2	SW / ISO Image	SLE-15-SP2-Full-aarch64-QU1-Media1.iso (SHA256: f04da5cf32448d2fafb5920175add0a42bfbacd0b6ff20303c793d46ee07dd4b)	SLES 15 SP2	Download
3	SW / ISO Image	SLE-15-SP2-Full-s390x-QU1-Media1.iso (SHA256: 00f6d37fcf910ebf039bf9b13ef85243610443a4183a3817a9ede8d389f0cee9)	SLES 15 SP2	Download
4	SW	openssh rpm package	8.1p1-5.18.1	Download and verification by the TOE
5	SW	openssh-helpers rpm package	8.1p1-5.18.1	Download and verification by the TOE
6	SW	openssh-fips rpm package	8.1p1-5.18.1	Download and verification by the TOE
7	SW	sudo rpm package	1.8.22-4.15.1	Download and verification by the TOE
8	SW	dnsmasq rpm package	2.78-7.6.1	Download and verification by the TOE
9	SW	permissions rpm package	20181224-23.3.1	Download and verification by the TOE
10	SW	audit rpm package	2.8.1-12.3.1	Download and verification by the TOE
11	SW	libaudit1 rpm package	2.8.1-12.3.1	Download and verification by the TOE
12	SW	libaudit1-32bit rpm package	2.8.1-12.3.1	Download and verification by the TOE
13	SW	libauparse0 rpm package	2.8.1-12.3.1	Download and verification by the TOE

No	Type	Identifier	Release	Form of Delivery
14	SW	python3-audit rpm package	2.8.1-12.3.1	Download and verification by the TOE
15	SW	audit-audispd-plugins rpm package	2.8.1-12.3.1	Download and verification by the TOE
16	SW	screen rpm package	4.6.2-5.3.1	Download and verification by the TOE
17	SW	libxml2-tools rpm package	2.9.7-3.34.1	Download and verification by the TOE
18	SW	libxml2-2 rpm package	2.9.7-3.34.1	Download and verification by the TOE
19	SW	python3-libxml2-python rpm package	2.9.7-3.34.1	Download and verification by the TOE
20	DOC	Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP2 [9] (SHA256: 5a904d61e8a9b7f016dc06a71791febf83d283fd1f2aad9216e5617e2155deee)	Version 0.10	Download

Table 2: Deliverables of the TOE

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

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 [6], chapter 4.2.

5. Architectural Information

SLES is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications. In addition, virtual machines provide an execution environment for a large number of different operating systems.

The AppArmor LSM is configured to enforce the authoritative access control policy. The following access control rules are enforced by enabled LSM:

- Isolation of virtual machines from each other by assigning each process implementing a virtual machine and its resources a unique label. Access between virtual machines and resources is only permitted if the label of the virtual machine and the accessed resource is identical.

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.

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.

5.1. TOE Structure and Security Functions

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.

The TOE provides the following security functionality:

Auditing

The Lightweight Audit Framework (LAF) is designed to be an audit system making Linux compliant with the requirements from Common Criteria. LAF is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem allows configuring the events to be actually audited from the set of all events that are possible to be audited.

The TOE can be deployed as an audit server that receives audit logs from other TOE instances. These audit logs are stored locally. The TOE provides search and review facilities to authorized administrators for all audit logs.

Cryptographic support

The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. For interactive usage, the SSHv2 protocol is provided. The TOE provides the server side as well as the client side applications. Using OpenSSH, password-based and public-key-based authentication are allowed.

In addition to OpenSSH, the TOE provides IPSec for a cryptographically secured communication with other remote entities. IPSec is offered together with IKEv2 for the key negotiating aspect. The implementations of IKEv2 allow a pre-shared key or certificate based authentication of the remote peer.

In addition, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt. Using this device mapper target, the Linux operating system offers administrators and users cryptographically protected block device storage space. With the help of a Password-Based Key-Derivation Function version 2 (PBKDF2) implemented with the LUKS mechanism, a user-provided passphrase protects the volume key which is the symmetric key for encrypting and decrypting data stored on disk. Any data stored on the block devices protected by dm_crypt is encrypted and cannot be decrypted unless the volume key for the block device is decrypted with the passphrase processed by PBKDF2. With the device mapper mechanism, the TOE allows for transparent encryption and decryption of data stored on block devices, such as hard disks.

Packet filter

The TOE provides a stateless and stateful packet filter for regular IP-based communication. OSI Layer 3 (IP) and OSI layer 4 (TCP, UDP, ICMP) network protocols can be controlled using this packet filter. To allow virtual machines to communicate with the environment, the TOE provides a bridging functionality. Ethernet frames routed through bridges are controlled by a separate packet filter which implements a stateless packet filter for the TCP/IP protocol family.

The packet filtering functionality offered by the TOE is hooked into the TCP/IP stack of the kernel at different locations. Based on these locations, different filtering capabilities are applicable. The lower level protocols are covered by the EBTables filter mechanism which includes the filtering of Ethernet frames including the ARP layer. The higher level protocols of TCP/IP are covered with the IPTables mechanism which allows filtering of IP and TCP, UDP, ICMP packets. In addition, IPTables offers a stateful packet filter for the mentioned higher level protocols.

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 or sudo command. These all rely on explicit authentication information provided interactively by a user.

The authentication security function allows password-based authentication. For SSH access, public-key-based authentication is also supported.

Password quality enforcement mechanisms are offered by the TOE which are enforced at the time when the password is changed.

Discretionary Access Control

DAC allows owners of named objects to control the access permissions to these objects. These owners can permit or deny access for other users based on the configured permission settings. The DAC mechanism is also used to ensure that untrusted users cannot tamper with the TOE mechanisms.

In addition to the standard Unix-type permission bits for file system objects as well as IPC objects, the TOE implements POSIX access control lists. These ACLs allow the specification of the access to individual file system objects down to the granularity of a single user.

Authoritative Access Control

The TOE supports authoritative or mandatory access control based on the following concept:

- To separate virtual machines and their resources at runtime, AppArmor rules are used. The virtual machine resources are labelled to belong to one particular virtual machine. In addition, a virtual machine is awarded a unique label. The TOE ensures that virtual machines can only access resources bearing the same label.

Virtual machine environments

The TOE implements the host system for virtual machines. It acts as a hypervisor which provides an environment to allow other operating systems to execute concurrently. AppArmor labels are attached to virtual machines and its resources. The access control policy is enforced using these labels to grant virtual machines access to resources if the category of the virtual machine is identical to the label of the accessed resource.

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.

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 test results provided by the developer were generated on the following systems:

- Intel (x86_64, Xeon)
- AMD (x86_64, EPYC)
- ARM (aarch64, ThunderX2)
- IBM (s390x, z15)

The software was installed and configured as defined in the Evaluated Configuration Guide (ECG) [9]. The test plan requires software packages to be installed for the test cases to be run properly. This is allowable since a) the package does not alter any TSF software, and b) it does not install any otherwise privileged software that would interact with the TSF that is being tested.

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 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 base for the testing and adapted them as needed. The test suites have a history in linux testing (their base versions are also available online). With regard to the audit-test suite, this is designed for use with an installed SELinux LSM in mind. The evaluator chose to deviate from the evaluated configuration and have the SELinux module active in permissive mode for the audit-test suite to run the tests that require SELinux to be present. All other tests including the AppArmor tests were run using the expected evaluated configuration setup.

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

Testing results

The test results were 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 are identical to the expected 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.

It should be noted that 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.

Conclusion

The evaluator has verified that developer testing was performed on hardware that is claimed in the ST.

The evaluator was able to follow and fully understand the developer testing approach by using the provided test documentation.

The evaluator analysed 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.

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 all automated test suites of the developer and the majority of the semi-automated (derived from the test suite) and manual tests. The evaluator tested on all supported TOE platforms.

The partial rerun of the test suite covered around 1600 tests.

The evaluator performed 18 additional tests in various areas.

Test approach and depth

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

- cryptographic algorithm coverage for IPsec, SSH, and dm-crypt
- DBus services
- special file systems, e.g. /sys
- failed authentication lockout and password obstruction
- potentially security-relevant commands not covered by developer tests
- AppArmor

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

TOE test configuration

The evaluator verified the test systems according to the documentation in the Evaluated Configuration Guide (ECG) [9] and the test plan and – as the ECG was evaluated to be consistent with the ST [6] – also with the ST.

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

Test results

All the test results conformed to the expected test results from the test plan.

7.3. Evaluator Penetration Testing

The evaluator performed 10 test cases.

Linux standard tools, fuzzers, and a CPU-vulnerability check program have been used as part of the testing.

Test approach and Depth

The evaluator used the public vulnerability databases and general search engines for finding publicly documented vulnerabilities. That lead to some tests in the areas of CPU checks and external network interfaces.

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: network, dbus services and programs.

In summary, the following aspects were subject to testing:

1. CPU vulnerabilities
2. Syscall interface
3. DBus services
4. Netlink message processing
5. undocumented security-relevant programs
6. access control to configuration files
7. unexpected network interfaces
8. unclear apparmor interface usage
9. mitigation of CVE entries

Configuration

The TOE was in its evaluated configuration as described in the Evaluated Configuration Guide (ECG) [9].

All supported platforms (Intel, AMD, ARM, s390) have been involved in the penetration testing. The documentation of the individual tests identified the specific platform used by the test.

Results

No deviation from the expected results has 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 processor: Delta D20x-M1-PC-32-8-96GB-1TB-2x1G
- x86 64bit AMD processor: AMD EPYC DP Server R181-Z90
- ARM processors: Gigabyte R181-T90
- IBM based on System z: IBM Z System z15

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

The Evaluation Methodology CEM [2] was used. For RNG assessment, the scheme interpretation 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 components 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 – Advanced Management, Version 2.0, 28 May 2010,
  OSPP Extended Package – Advanced Audit, Version 2.0, 28 May 2010,
  OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010 [8]
- 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 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The tables 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. No Cryptographic Functionality in those tables is already known to not achieve at least a security level of 100 Bits (in general context).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of

Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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

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

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
ACL	Access Control List
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ECG	Evaluated Configuration Guide
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KVM	Kernel Virtualized Machine

LSM	Linux Security Module
LUKS	Linux Unified Key Setup
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
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
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 licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

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

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1151-2021, Version 3.02, 29 April 2021, Security Target for SUSE Linux Enterprise Server 15 SP2 including KVM virtualization, SUSE Software Solutions Germany GmbH

[7] Evaluation Technical Report, Version 7, 02 July 2021, Final Evaluation Technical Report, atsec information security 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

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

[9] Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP2, Version 0.12, 09 June 2021

[10] Linux Specification High-level design – Linux Kernel and User Space – SUSE Linux Enterprise Server 15, 16 November 2020

[11] Configuration list for the TOE, 10 June 2021, MASTER CM List (confidential document)

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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex C of Certification Report BSI-DSZ-CC-1151-2021

Overview of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
0	Authentication	The client authenticates either with UserID & password (#3) or by cryptographic means as shown in #1 and #2 and verified by the server respectively.			
1		RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-2	[RFC3447], PKCS#1 v2.1 sec.8.2 (RSA) [FIPS180-4] (SHA) [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	Modulus length: 2048, 3072 and 4096	Pubkeys are exchanged trustworthy out of band, e.g. checking fingerprints. Authenticity is not part of the TOE. (no certificates are used)
2		ECDSA signature generation and verification using SHA-{256, 384, 512} on nistp-{256, 384, 521} (ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521)	[ANSI X9.62] (ECDSA), [FIPS180-4] (SHA), NIST curves [FIPS186-4] identifiers analogous to [RFC5903], sec 5 [RFC5656] secp{256,384,521}r1 [SEC2] [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	plength=256, 384, 521 depends on selected curve	
3		User name and password-based authentication	[RFC4252], sec. 5 (SSH-AUTH) for user authentication	Guess success prob. $\varepsilon \leq 2^{-20}$	PAM is used centrally. Thus if the authentication is aborted the counter for failed logins is

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
					increased and remains as is for the next login.
4	Key agreement (key exchange)	DH with diffie-hellman-group-exchange-sha256	[RFC4253] (SSH-TRANS) supported by [RFC4419] (DH-Group Exchange) [FIPS-180-4] (SHA)	plength= 2K, 3K, 4K, etc.	As of /etc/ssh/moduli
5		ECDH with ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521 (ecdh-sha2-nistp256 ecdh-sha2-nistp384, ecdh-sha2-nistp521)	[RFC4253] (SSH-TRANS) [FIPS-180-4] (SHA) supported by [RFC5656] (ECC in SSH) secp{256,384,521}r1 [SEC2] NIST curves [FIPS186-4] identifiers analogous to [RFC5903], sec 5	plength=256, 384, 521 depends on selected curve	
6	Confidentiality	AES in CBC mode, and CTR mode (aes128-cbc, aes192-cbc, aes256-cbc) (aes128-ctr, aes192-ctr, aes256-ctr);	[FIPS197] (AES), [SP 800-38A] (CBC), [RFC 4253] (SSH-TRANS using AES with CBC mode), [RFC4344] (SSH-2 using AES with CTR mode)	|k|=128, 192, 256	
7	Integrity and Authenticity	HMAC-SHA-2 (hmac-sha2-256, hmac-sha2-512)	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support)	|k|= 256, 512	BPP: Message authentication
8	Authenticated encryption (encrypt-then authenticate)	HMAC-SHA-1 (hmac-sha1-etm@openssh.com) HMAC-SHA-2 (hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com) + CBC-AES	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support), [RFC6668] (SHA-2 in SSH)	|k|=160, 256, 512	etm = encrypt-then-MAC (OpenSSH 6.2)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
9		AES in GCM mode (aes128-gcm@openssh.com, aes256-gcm@openssh.com)	[RFC5647]	|k|=128, 256	
10	Key generation for host and user keys	RSA key generation with key size: 2048, 3072, 4096 bits	[FIPS 186-4], B.3.3 and C.3 for Miller Rabin primality tests.	n/a	Using FCS_RNG.1(SSL)
11		ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS 186-4], B.4	n/a	
12	Key generation for diffie-hellman key agreement	DSA key generation with key size: 2048, 3072, 4096, 6144, 8192 bits	[SP800-56A-Rev3], sec. 5.6.1.1.4 [RFC4253] [RFC4306]	n/a	Using FCS_RNG.1(SSL)
13		ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[SP800-56A-Rev.3], sec. 5.6.1.2.2 [RFC4253] [RFC4306]	n/a	
14	Trusted channel	FTP_ITC.1 a) [ST], sec. 6.2.1.45 for SSHv2.0	Cf. all lines above	See above	

Table 3: TOE cryptographic functionality for SSH

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Authenticity	RSA signature verification (RSASSA-PSS) using SHA-256 and SHA-384	[RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 2048, 3072 and 4096	Verification of certificate signatures provided for authentication Server and client certificates are used. Algorithms used depending on the signature algorithm* / hash functions** used for signing the certificates

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
2		RSA signature verification (RSASSA-PKCS1-v1.5) using SHA-256, SHA-384, SHA-512	[RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 2048, 3072 and 4096	
3		ECDSA signature verification using SHA-256, SHA-384, SHA-512 on P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), EC secp{256, 384, 521}r1 [SEC2]	Key sizes corresponding to the used elliptic curve plength=256, 384, 521	Only NIST curves NIST P-256, NIST P-384, or NIST P-521 are allowed – see ECG [9]. Recommen-dation use for signatures of certificates: SHA-256 on P-256 curve SHA-384 on P-384 curve SHA-521 on P-521 curve if any.
4	IKE authentication	RSA signature generation and verification RSASSA-PSS using SHA-256 and SHA-384 (Auth Method 14)	[RFC5996] (IKEv2) [RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 2048, 3072 and 4096	
5		RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-256, SHA-384, SHA-512 (Auth Method 1)	analogous to [RFC7427] [RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 2048, 3072 and 4096	
6		ECDSA signature generation and verification with SHA-256 on P-256 curve SHA-384 on P-384 curve SHA-521 on P-521 curve (Auth Method 9, 10, 11)	[FIPS 186-4] [FIPS180-4](SHA) [RFC4754] (IKEv2 using ECDSA), EC secp{256, 384, 521}r1 [SEC2]	Key sizes corresponding to the used elliptic curve plength =256, 384, 521	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
7	IKE key agreement	DH with DH groups based on ECC	[RFC5996] (IKEv2), [DH] (DH as referenced in [RFC5996])		
8		MODP groups: exponentiation groups modulo a prime	[RFC3526] groups 14, 15, 16, 17,18 (2048, 3072, 4096, 6144, 8192)-bit MODP groups	Plength= 2048, 3072, 4096, 6144, 8192	
9	IKE key derivation	PRF based on: HMAC-SHA1 (ID 2 PRF_HMAC_SHA1) 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)	[RFC5996] (IKEv2), [FIPS198-1] (HMAC), [FIPS180-4] (SHA) [RFC4868] (HMAC -SHA2 with IPsec) [IKEV2IANA]	|k| = variable[8]	IKE keys (IKE SA) and IPsec keys (IPsec SA / child SA) are derived according to the key length required for the negotiated algorithms they are used for.[9]
10	IKE integrity and authenticity and IPsec ESP integrity and authenticity	HMAC with SHA1 (ID7 AUTH_HMAC_SHA1_160) HMAC with SHA-256-128 (ID 12 AUTH_HMAC_SHA2_256_128) HMAC with SHA-384-192 (ID 13 AUTH_HMAC_SHA2_384_192) HMAC with SHA-512-256 (ID 14 AUTH_HMAC_SHA2_512_256)	[RFC 5996], [RFC4307] (IKEv2) [FIPS180-4] (SHA), [FIPS198-1] (HMAC), [RFC4868] (HMAC -SHA2 with IPsec) [RFC2404] (HMAC using truncated SHA-1) [IKEV2IANA] [RFC4595] (HMAC-SHA-1)	|k|=160, 256, 384, 512	

[8] preferred keysize = size of the output of the underlyin 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	Comments
11	IKE encryption and IPsec ESP encryption	AES in CBC mode (ID 12 ENCR_AES_CBC)	[RFC5996], [RFC3602] supported by [RFC4307]	|k|=128, 192, 256	
12		AES in CTR mode (ID 13 ENCR_AES_CTR)	[RFC5930], [RFC3686] supported by [RFC4307]	|k|=128, 192, 256	
13	IKE authenticated encryption and IPsec ESP authenticated encryption	AES in CCM mode (ID 14 ENCR_AES-CCM_8) (ID 15 ENCR_AES-CCM_12) (ID 16 ENCR_AES-CCM_16)	[RFC5282], [RFC4309], [RFC5116]	|k|=128, 192, 256	AEAD
14		AES in GCM mode (ID 18 AES-GCM with a 8 octet ICV) (ID 19 AES-GCM with a 12 octet ICV) (ID 20 AES-GCM with a 16 octet ICV)	[RFC5282], [RFC4106], [RFC5116]	|k|=128, 192, 256	
15	Key generation	RSA key generation with key size: 2048, 3072, 4096 bits	[FIPS 186-4], B.3.3 and C.3 for Miller Rabin primality tests.	n/a	Keys for certificates and for certificate signing Using either FCS_RNG.1 (SSL)
16		ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS 186-4], B.4	n/a	
17	Trusted Channel	FTP_ITC.1 b), [ST] sec. 6.2.1.47 for IKEv2, IPsec ESP	Cf. all lines above, especially [RFC5996] (IKEv2) [RFC4303] (ESP)	See above	Either in transport mode or in tunnel mode

Table 4: TOE cryptographic functionality for IPSec

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Key derivation with authentication (access control, protection / recovery mode)	Password based key derivation using PBKDF2 with PRF HMAC using SHA-1, SHA-256, SHA-384, SHA-512	[SP800-132] [CFLUKS][10] [RFC2898] (PBKDF2] [FIPS198-1] (HMAC) [FIPS180-4](SHA)	Guessing prob. 2^{-20} Salt 32 byte (LUKS_SALTSIZE) iteration count 1000 ms	
2	Confidentiality (bulk data & key access / key wrapping)	AES in XTS mode IV-handling mechanism: XTS-plain64 XTS-benbi	[FIPS197] [SP800-38E] (XTS)	|k|= 2*128, 2*192, 2*256	

Table 5: TOE cryptographic functionality for dm-crypt

References for Table 3 to 5

ANSI X9.62 Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA)
Date 16 November 2005
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/publications/detail/fips/180/4/final

FIPS186-4 Digital Signature Standard (DSS)
Date 2013-07-19
Location https://csrc.nist.gov/publications/detail/fips/186/4/final

FIPS197 Advanced Encryption Standard (AES)
Date 2001-11-26
Location https://csrc.nist.gov/publications/detail/fips/197/final

IKEV2IANA Internet Key Exchange Version 2 (IKEv2) Parameters
Date 2021-02-16
Location https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xml

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

RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
Author(s) C. Madson, R. Glenn
Date 1998-11-01
Location http://www.ietf.org/rfc/rfc2404.txt

RFC3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
Author(s) J. Jonsson, B. Kaliski
Date 2003-02-01
Location http://www.ietf.org/rfc/rfc3447.txt

[10] Please note that the master key of [CFLUKS] is called DPK in [SP800-132] and in [SP800-132] the Master key is called the key which is derived from the user password.

RFC3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
Author(s) T. Kivinen, M. Kojo
Date 2003-05-01
Location http://www.ietf.org/rfc/rfc3526.txt

RFC3602 The AES-CBC Cipher Algorithm and Its Use with Ipsec
Author(s) S. Frankel, R. Glenn, S. Kelly
Date 2003-09-01
Location http://www.ietf.org/rfc/rfc3602.txt

RFC4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
Author(s) J. Viega, D. McGrew
Date 2005-06-01
Location http://www.ietf.org/rfc/rfc4106.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

RFC4303 IP Encapsulating Security Payload (ESP)
Author(s) S. Kent
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4303.txt

RFC4306 Internet Key Exchange (IKEv2) Protocol
Author(s) C. Kaufman
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4306.txt

RFC4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
Author(s) J. Schiller
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4307.txt

RFC4309 Using Advanced Encryption Standard (AES) CCM Mode with Ipsec Encapsulating Security Payload (ESP)
Author(s) R. Housley
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4309.txt

RFC4344 The Secure Shell (SSH) Transport Layer Encryption Modes
Author(s) M. Bellare, T. Kohno, C. Namprempre
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4344.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

RFC4595 Use of IKEv2 in the Fibre Channel Security Association Management Protocol
Author(s) F. Maino, D. Black
Date 2006-07-01
Location http://www.ietf.org/rfc/rfc4595.txt

RFC4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
Author(s) D. Fu, J. Solinas
Date 2007-01-01
Location http://www.ietf.org/rfc/rfc4754.txt

RFC4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
Author(s) S. Kelly, S. Frankel
Date 2007-05-01
Location http://www.ietf.org/rfc/rfc4868.txt

RFC5116 An Interface and Algorithms for Authenticated Encryption
Author(s) D. McGrew
Date 2008-01-01
Location http://www.ietf.org/rfc/rfc5116.txt

RFC5282 Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
Author(s) D. Black, D. McGrew
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5282.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 AlgorithmIntegration 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

RFC5930 Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol
Author(s) S. Shen, Y. Mao, NSS. Murthy
Date 2010-07-01
Location http://www.ietf.org/rfc/rfc5930.txt

RFC5996 Internet Key Exchange Protocol Version 2 (IKEv2)
Author(s) C. Kaufman, P. Hoffman, Y. Nir, P. Eronen
Date 2010-09-01
Location http://www.ietf.org/rfc/rfc5996.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

RFC7427 Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
Author(s) T. Kivinen, J. Snyder
Date 2015-01-01
Location http://www.ietf.org/rfc/rfc7427.txt

SEC2 Recommended Elliptic Curve Domain Parameters
Date 2000
Location http://www.secg.org

SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques
Date 2001-12-01
Location https://csrc.nist.gov/publications/detail/sp/800-38a/final

SP 800-38E Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices
Date 2010-01-18
Location https://csrc.nist.gov/publications/detail/sp/800-38e/final

Note: End of report