Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1168-2021

for

SUSE Linux Enterprise Server, Version 15 SP2

from

SUSE LLC

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1168-2021 (*)

Operating Systems

SUSE Linux Enterprise Server
Version 15 SP2

from	SUSE LLC
PP Conformance:	Protection Profile for General Purpose Operating Systems Version 4.2.1, 22 April 2019, CCEVS-VR-PP-0047, NIAP, Extended Package for Secure Shell (SSH), Version 1.0, 19 February 2016, CCEVS-VR-PP-0039, NIAP
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 extended

SOGIS
Recognition Agreement
for components up to
EAL 4

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, 11 November 2021

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - 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 licencing process (CC-Stellen) [3]

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 Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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. 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 10 November 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 LLC.

The product was developed by: SUSE LLC.

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

5. Validity of the Certification Result

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

- all stipulations regarding generation, configuration and operation, as given in the 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

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 11 November 2021 is valid until 10. November 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,
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 LLC
10 Canal Park, Suite 200
Cambridge, MA 02141
USA

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 for General Purpose Operating Systems Version 4.2.1, 22 April 2019, CCEVS-VR-PP-0047, NIAP [8] and an Extended Package [11]:

- Extended Package for Secure Shell (SSH), Version 1.0, 19 February 2016, CCEVS-VR-PP-0039, NIAP.

The TOE Security Assurance Requirements (SAR) relevant for the TOE are outlined in the Security Target [6], chapter 6.3. They are selected from Common Criteria Part 3 and there is one additional Extended Component defined in the Protection Profile. Thus the TOE is CC Part 3 extended. The TOE meets the assurance requirements defined in the Protection Profile.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
Audit	The 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 support	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. ● dm_crypt: 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. ● OpenSSL: the TOE offers the TLS protocol to protect network links to remote systems. The TLS protocol stack can be used as TLS client.

TOE Security Functionality	Addressed issue
	The cryptographic primitives for implementing the above mentioned cryptographic communication protocols are provided by OpenSSL.
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.
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.

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 and Threats. This is outlined in the Security Target [6] chapters 3.1 and 3.2.

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

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 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	D/L
2	SW/ ISO Image	SLE-15-SP2-Full-aarch64-QU1-Media1.iso (SHA256: f04da5cf32448d2fafb5920175add0a42bfbacd0b6ff20303c793d46ee07dd4b	SLES 15 SP2	D/L
3	SW/ ISO Image	SLE-15-SP2-Full-s390x-QU1-Media1.iso (SHA256: 00f6d37fcf910ebf039bf9b13ef85243610443a4183a3817a9ede8d389f0cee9	SLES 15 SP2	D/L
4	DOC	Common Criteria Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP2 (NIAP) (SHA256: 73dd8a8d47228838d65e9a4440dc6267d634a051d9befec4abd72c3e5968da39)	SLES 15 SP2, Document version 0.16	D/L
5	SW	openssh	8.1p1-5.18.1	D/L and verification through TOE
6	SW	openssh-helpers	8.1p1-5.18.1	D/L and verification through TOE
7	SW	openssh-fips	8.1p1-5.18.1	D/L and verification through TOE
8	SW	openssl-1_1	1.1.1d-11.20.1	D/L and verification through TOE
9	SW	sudo	1.8.22-4.15.1	D/L and verification through TOE
10	SW	dnsmasq	2.78-7.6.1	D/L and verification through TOE
11	SW	permissions	20181224-23.3.1	D/L and verification through TOE
12	SW	kernel-default	5.3.18-24.78.1	D/L and verification through TOE
13	SW	audit	2.8.1-12.3.1	D/L and verification through TOE
14	SW	libaudit1	2.8.1-12.3.1	D/L and verification through TOE
15	SW	libauparse0	2.8.1-12.3.1	D/L and verification through TOE

No.	Type	Identifier	Release	Form of Delivery
16	SW	python3-audit	2.8.1-12.3.1	D/L and verification through TOE
17	SW	audit-audispd-plugins	2.8.1-12.3.1	D/L and verification through TOE
18	SW	screen	4.6.2-5.3.1	D/L and verification through TOE
19	SW	libxml2-tools	2.9.7-3.34.1	D/L and verification through TOE
20	SW	libxml2-2	2.9.7-3.34.1	D/L and verification through TOE
21	SW	python3-libxml2-python	2.9.7-3.34.1	D/L and verification through TOE
22	SW	grub2	2.04-9.45.2	D/L and verification through TOE
23	SW	grub2-systemd-sleep-plugin	2.04-9.45.2	D/L and verification through TOE
24	SW	grub2-snapper-plugin	2.04-9.45.2	D/L and verification through TOE
25	SW	libaudit1-32bit	2.8.1-12.3.1	D/L and verification through TOE
26	SW	shim	15.4-3.20.1	D/L and verification through TOE
27	SW	grub2-x86_64-efi	2.04-9.45.2	D/L and verification through TOE
28	SW	grub2-i386-pc	2.04-9.45.2	D/L and verification through TOE
29	SW	s390-tools	2.11.0-9.31.1	D/L and verification through TOE
30	SW	grub2-s390x-emu	2.04-9.45.2	D/L and verification through TOE
31	SW	grub2-arm64-efi	2.04-9.45.2	D/L and verification through TOE
32	SW	cpio	cpio-2.12-3.9.1	D/L and verification through TOE
33	SW	polkit	polkit-0.116-3.3.1	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 ISO-Images and additional rpm packages. 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 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, Identification and Authentication, Discretionary Access Control 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:

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

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.

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 includes a set of trusted processes, which when called 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 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.

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, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt.

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

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. 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.

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 evaluator tested on hardware setup defined in the ST:

- x86 64bit Intel Xeon processors: Delta D20x-M1-PC-32-8-96GB-1TB-2x1G
- x86 64bit AMD processors: AMD EPYC DP Server R181-Z90
- ARM processors: Gigabyte R181-T90
- IBM based on System z: IBM Z System z15

All tests were performed on all hardware platforms. The evaluated configuration is specified in chapter 8 of this report.

7.1. Evaluator Independent Testing

The evaluator performed all the tests defined in the PP [8] and SSH-EP [11], which makes it around 100 tests. For the test requirements on crypto primitives and RNG, the CACS ACVP tests were performed on all applicable cryptographic algorithms. The evaluator tests are partly manual tests, and partly automated. The evaluator executed tests on the TOE, most notably kernel version 5.3.18-24.78-default.

Three types of tests were performed - independent testing as defined by the Protection Profile [8] and the Extended Package [11], entropy tests, and CAVS algorithm testing:

Independent testing

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

- key destruction test: this test includes the modification of a test client to determine the used keys, with a subsequent search through the TOE physical memory.
- stack protection: a tool has been used that analyses the binary file meta data to determine whether stack protection is enforced
- communication modification: proxy setups where deployed in order to modify live-traffic to exercise the TOE behavior for situations where the TLS protocol is violated

Algorithm testing

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

Entropy tests

A modified version of the kernel with an additional interface was used to be able to gather raw entropy data from the kernel.

No deviation from the expected results have been encountered.

7.2. 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.

The evaluator used the MITRE CVE portal, SUSE support center, and Google searches to find publicly documented vulnerabilities. This lead to some tests in the areas of CPU checks and external network interfaces.

In summary, the following aspects were subject to testing:

1. Unmitigated OS-relevant CPU vulnerabilities
2. Potentially inappropriately controlled DBus services
3. Potentially insecure netlink message processing
4. Undocumented security-relevant programs
5. Potentially inappropriate access control to configuration files
6. Unexpected network interfaces
7. Potential chrony vulnerability
8. General privilege escalation scan

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 Xeon processors: Delta D20x-M1-PC-32-8-96GB-1TB-2x1G
- x86 64bit AMD processors: AMD EPYC DP Server R181-Z90
- ARM processors: Gigabyte R181-T90
- IBM based on System z: IBM Z System z15

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used.

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

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components claimed in the Security Target [6], chapter 6.3 and defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: Protection Profile for General Purpose Operating Systems Version 4.2.1, 22 April 2019, CCEVS-VR-PP-0047, NIAP, Extended Package for Secure Shell (SSH), Version 1.0, 19 February 2016, CCEVS-VR-PP-0039, NIAP
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 extended

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 give 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 100 Bits*' of the tables in annex C of part D with '*no*' achieves a security level of lower than 100 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 [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
ACVP	Automated Cryptographic Validation Program
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation

cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ECG	Evaluated Configuration Guide
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TLS	Transport Layer Security

12.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

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-1168-2021, Version 0.15, 2021-08-27, Security Target for SUSE Linux Enterprise Server 15 SP2 NIAP OSPP Compliance, SUSE LLC

[7] Evaluation Technical Report, Version 5, 2021-11-09, Final Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] Protection Profile for General Purpose Operating Systems Version 4.2.1, 22 April 2019, CCEVS-VR-PP-0047, NIAP

[9] Common Criteria NIAP Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP2 (NIAP), Version 0.16, 2021-09-22

[10] Configuration list for the TOE, 2021-10-01, MASTER CM List (confidential document)

[11] Extended Package for Secure Shell (SSH), Version 1.0, 19 February 2016, CCEVS-VR-PP-0039, NIAP

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 9, 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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex C of Certification Report BSI-DSZ-CC-1168-2021

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 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-PKC-S1-v1.5 using SHA-2 (rsa-sha2-256 or rsa-sha2-512)	[RFC3447], PKCS#1 v2.1sec.8.2(RSA) [FIPS180-4] (SHA) [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7(SSH-AUTH) for user authentication	Modulus length: 2048, 3072and 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		ECDSA signature generation and verification using SHA-{256, 384, 512} on nistp-{256, 384, 521} (ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,ecdsa-sha2-nistp521)	[ANSIX9.62] (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	plength=256, 384, 521 depends on selected curve	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
			user authentication			
3		User name and password-based authentication	[RFC4252], sec. 5 (SSH-AUTH) for user authentication	Guess success prob. ε ≤ 2 -20	yes	PAM is used centrally. Thus if the authen-tication is aborted the counter for failed logins is 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.	yes	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	yes	
6	Confidentiality	AES in CBC mode, and CTR mode (aes128-cbc, aes192-cbc, aes256-cbc) (aes128-ctr, aes192-ctr, aes256-ctr);	[FIPS197] (AES), [SP800-38A] (CBC), [RFC 4253] (SSH-TRANS using AES with CBC mode), [RFC4344] (SSH-2 using AES with CTR mode)	|k|=128, 192, 256	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
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	yes	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	yes	etm = encrypt-then-MAC(OpenSSH 6.2)
9		AES in GCM mode(aes128-gcm@openssh.com, aes256-gcm@openssh.com)	[RFC5647]	|k|=128, 256	yes	
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	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	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	n/a	Using FCS_RNG.1(SSL)
13		ECDSA key generation based on the NIST curves:	[SP800-56A-Rev.3], sec. 5.6.1.2.2 [RFC4253]	n/a	n/a	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		P-256, P-384, and P-521	[RFC4306]			
14	Trusted channel	FTP_ITC.1 a) [ST], sec. 6.2.1.45 for SSHv2.0	Cf. all lines above	See above	yes	

Table 3: TOE cryptographic functionality for SSH

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Confidentiality	Cipher: AES Modes: CBC, GCM	CBC: [RFC5246], SP800-38A GCM: [RFC5288], [SP800-38D]	128, 256	yes	-
2	Integrity and authenticity	HMAC SHA-1 HMAC SHA-256 HMAC-SHA-384 AES GMAC used by GCM	[RFC5246] FIPS180-4 (SHA) [FIPS198] (HMAC) SP800-38D (GCM / GMAC)	Key length equal to digest	yes	-
3	Key Agreement	DH with PQG: MODP Group 14, MODP Group 15, MODP Group 16, MODP Group 17, MODP Group 18 ECDH with curves NIST P-256, NIST P- 384, NIST P-521	RFC5246, SP800-56A rev 3	Keys size as defined by PQG parameters / curves	n/a	-
4	IV / Key derivation	PRF MD-5/SHA-1, SHA-2 with hash type chosen by TLS cipher suite	RFC5246 FIPS 180-4 FIPS 198	Depending on chosen cipher, compliant to RFC5246	yes	-
5	Peer authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-1 and SHA-2	RFC 5246 FIPS 186-4 FIPS 180-4 RFC3447, (PKCS#1v2.1) Sec. 8 (RSA)	Modulus >= 2048 bits Keys size as defined by curves	yes	-
		RSA signature generation and				

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		verification RSASSA- PSS using SHA-1 and SHA-2				
		ECDSA with signature generation and verification using SHA- 1 and SHA-2 with NIST P-256, P-384, P-521	RFC5246 Sec1-v2 (ECDSA) ([SEC2]) FIPS180-4 (SHA)			
6	Key generation for authentication	ECDSA using NIST P-256, P-384, P-521	FIPS 186-4, B.4	Modulus >= 2048 bits Keys size as defined by curves	yes	-
		RSA with 1024, 2048, 3072, 4096 bits 5 (2048 bits and lower), 4 (larger key sizes) rounds of Miller-Rabin	FIPS 186-4, B.3.3 and C.3 for Miller primality tests			
7	Key generation for DH / ECDH	DSA using PQG parameter set defined for DH operation	SP800-56A rev. 3 section 5.6.1.1.4 RFC5246	Keys size as defined by PQG parameters	n/a	-
		ECDSA with NIST P-256, P-384, P-521	SP800-56A rev. 3 section 5.6.1.2.2 RFC5246	Keys size as defined by curves		
8	Trusted channel	FTP_ITC.1 ST, Section 6.1.1.10 TLS	See listed above	-	n/a	-
9	Random number generator	CTR DRBG with AES- 256, with DF, without PR	[SP800-90A-Rev1]	-	n/a	-

Table 4: TOE cryptographic functionality for TLS

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Key derivation with authentication (access control,	Password based key derivation using PBKDF2 with PRF HMAC using SHA-1,	[SP800-132] [CFLUKS]6 Please note that the master key of	Guessing prob. 2 -20 Salt 32 byte (LUKS_SALSIZE)	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
	protection / recovery mode)	SHA-256, SHA-384, SHA-512	[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. [RFC2898] (PBKDF2] [FIPS198-1] (HMAC), [FIPS180-4] (SHA)	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	yes	

Table 5: TOE cryptographic functionality for dm-crypt

References for Table 3 to 5:

ANSIX9.62 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

FIPS198 FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC)
Date July 2008
File name adv/NIST.FIPS.198-1.pdf

RFC0768 User Datagram Protocol

Author(s) J. Postel

Date 1980-08-01

Location http://www.ietf.org/rfc/rfc0768.txt

RFC0791 Internet Protocol

Author(s) J. Postel

Date 1981-09-01

Location http://www.ietf.org/rfc/rfc0791.txt

RFC0792 Internet Control Message Protocol

Author(s) J. Postel

Date 1981-09-01

Location http://www.ietf.org/rfc/rfc0792.txt

RFC0793 Transmission Control Protocol

Author(s) J. Postel

Date 1981-09-01

Location http://www.ietf.org/rfc/rfc0793.txt

RFC0826 An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware

Author(s) D. Plummer

Date 1982-11-01

Location http://www.ietf.org/rfc/rfc0826.txt

RFC0903 A Reverse Address Resolution Protocol

Author(s) R. Finlayson, T. Mann, J.C. Mogul, M. Theimer

Date 1984-06-01

Location http://www.ietf.org/rfc/rfc0903.txt

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

RFC2119 Key words for use in RFCs to Indicate Requirement Levels

Author(s) S. Bradner

Date 1997-03-01

Location http://www.ietf.org/rfc/rfc2119.txt

RFC2367 PF_KEY Key Management API, Version 2

Author(s) D. McDonald, C. Metz, B. Phan

Date 1998-07-01

Location http://www.ietf.org/rfc/rfc2367.txt

RFC2401 Security Architecture for the Internet Protocol

Author(s) S. Kent, R. Atkinson

Date 1998-11-01

	Location	http://www.ietf.org/rfc/rfc2401.txt
RFC2460	Internet Protocol, Version 6 (IPv6) Specification	
	Author(s)	S. Deering, R. Hinden
	Date	1998-12-01
	Location	http://www.ietf.org/rfc/rfc2460.txt
RFC3376	Internet Group Management Protocol, Version 3	
	Author(s)	B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan
	Date	2002-10-01
	Location	http://www.ietf.org/rfc/rfc3376.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
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
RFC4301	Security Architecture for the Internet Protocol	
	Author(s)	S. Kent, K. Seo
	Date	2005-12-01
	Location	http://www.ietf.org/rfc/rfc4301.txt
RFC4306	Internet Key Exchange (IKEv2) Protocol	
	Author(s)	C. Kaufman
	Date	2005-12-01
	Location	http://www.ietf.org/rfc/rfc4306.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
RFC5246	The Transport Layer Security (TLS) Protocol Version 1.2	
	Author(s)	T. Dierks, E. Rescorla

	Date	2008-08-01
	Location	http://www.ietf.org/rfc/rfc5246.txt
RFC5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS	
	Author(s)	J. Salowey, A. Choudhury, D. McGrew
	Date	2008-08-01
	Location	http://www.ietf.org/rfc/rfc5288.txt
RFC5647	AES Galois Counter Mode for the Secure Shell Transport Layer Protocol	
	Author(s)	K. Igoe, J. Solinas
	Date	2009-08-01
	Location	http://www.ietf.org/rfc/rfc5647.txt
RFC5656	Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer	
	Author(s)	D. Stebila, J. Green
	Date	2009-12-01
	Location	http://www.ietf.org/rfc/rfc5656.txt
RFC5903	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2	
	Author(s)	D. Fu, J. Solinas
	Date	2010-06-01
	Location	http://www.ietf.org/rfc/rfc5903.txt
RFC6668	SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol	
	Author(s)	D. Bider, M. Baushke
	Date	2012-07-01
	Location	http://www.ietf.org/rfc/rfc6668.txt
SP800-38A	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
SP800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	
	Date	2007-11-28
	Location	https://csrc.nist.gov/publications/detail/sp/800-38d/final
SP800-38E	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
SP800-56A-Rev3	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography	
	Date	2018-04-16
	Location	https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
SP800-90A-Rev1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	
	Date	2015-06-24
	Location	https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final

Note: End of report