Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1213-2023

for

SUSE Linux Enterprise Server Version 15 SP4

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-1213-2023 (*)

Operating System

SUSE Linux Enterprise Server, Version 15 SP4

from	SUSE LLC
PP Conformance:	Protection Profile for General Purpose Operating Systems Version 4.2.1, 22 April 2019, CCEVS-VR-PP-0047, NIAP, Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 extended ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_INT.1, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1
valid until:	14 December 2028

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.

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

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

Bonn, 15 December 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Director-General

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 und für Heimat (Federal Ministry of the Interior and Community)
- 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 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.

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

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

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

4. Performance of Evaluation and Certification

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

The product SUSE Linux Enterprise Server, Version 15 SP4 has undergone the certification procedure at BSI.

The evaluation of the product SUSE Linux Enterprise Server, Version 15 SP4 was conducted by atsec information security GmbH. The evaluation was completed on 12 December 2023. 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 maximum validity of the certificate has been limited. The certificate issued on 15 December 2023 is valid until 14 December 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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

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

6. Publication

The product SUSE Linux Enterprise Server, Version 15 SP4 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
1221 S Valley Grove Way
#500, Pleasant Grove, UT 84062
United States

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is SUSE Linux Enterprise Server, 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] supplemented by the Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP [9].

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 TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified by the requirements. Each audit record contains the date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event.
Cryptographic support	The TOE includes the OpenSSL version 1.1.1 cryptographic libraries for performing userspace cryptographic operations. In addition, the Linux kernel crypto API performs the cryptographic operations performed by the kernel. In addition, the TOE uses software noise sources for entropy generation. The TOE implements TLSv1.2 for secure communications with remote servers. The TOE implements SSHv2 for allowing secure remote administration.
User data protection	The TOE implements access controls which can be configured to prevent unprivileged users from accessing files and directories owned by other users. The configuration of the access control mechanism is left to the owner of the file system object.
Identification and Authentication	All users including administrators must be authenticated to the TOE prior to carrying out any actions, including management operations. The TOE supports password-based authentication, authentication based on SSH-keys as well as X.509 certificate-based authentication. The TOE will lock out user accounts after a defined number of unsuccessful authentication attempts to that user account has been met.
Security Management	The TOE can perform management functions. The administrator has full access to carry-out all management functions offered by the TOE. The user is allowed a limited set of administrative operations for his own user account.
Protection of the TSF	The TOE implements the following protection of TSF data functions:

TOE Security Functionality	Addressed issue
	● Access controls ● Address space layout randomization (ASLR) with 11 bits (stack) and 28 bits (text segment start address) of entropy ● Stack buffer overflow protection ● Verification of integrity of the boot-chain ● Trusted software updates using digital signatures
TOE Access	The TOE displays an advisory warning message regarding unauthorized use of the OS prior to establishment of a user session.
Trusted Path / Channel	The TOE supports TLS v1.2 for trusted channel communications. The TOE uses TLS to securely communicate with the SUSE Customer Center. Applications may invoke the TOE-provided TLS to securely communicate with remote servers. The TOE offers an SSH server which uses the SSHv2 protocol allowing remote administration.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.2.

The TOE Security Problem Definition has been taken from the Protection Profile [8] and is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapter 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 SP4

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW (ISO image)	SLE-15-SP4-Full-x86_64-QU3-Media1.iso (SHA-256: 447baa21dd85e5433a1a2b2f46fe91491e8792f559397aca86fdf7a114c23c06)	SLES 15 SP4	D/L

No	Type	Identifier	Release	Form of Delivery
2	SW (ISO image)	SLE-15-SP4-Full-aarch64-QU3-Media1.iso (SHA-256: 664f17cf0d853ffdaca8781670249cd39213e9cfcc64e1de4318b6a5e9bb0eff)	SLES 15 SP4	D/L
3	SW (ISO image)	SLE-15-SP4-Full-s390x-QU3-Media1.iso (SHA-256: 60a4e8306cbdbe693353fb85836c04e0267ca64cd1adbb40f405f2708027cfe4)	SLES 15 SP4	D/L
4	SW (ISO image)	SLE-15-SP4-Full-ppc64le-QU3-Media1.iso (SHA-256: afd6a7843da52ffa8c44e0f0c1567a141a331fbe4ee3f2bd16eaac43cbaa65bb)	SLES 15 SP4	D/L
5	DOC	Common Criteria Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP4 (SHA-256: c1e0abfee4412e312ea440041bd737a72b2a4e4846503551e32446f14962ac58)	SLES 15 SP4, version 4.0	D/L
6	SW (rpm package)	openssh	8.4p1-150300.3.22.1	D/L and verification by the TOE
7	SW (rpm package)	openssh-client	8.4p1-150300.3.22.1	D/L and verification by the TOE
8	SW (rpm package)	openssh-common	8.4p1-150300.3.22.1	D/L and verification by the TOE
9	SW (rpm package)	openssh-fips	8.4p1-150300.3.22.1	D/L and verification by the TOE
10	SW (rpm package)	openssh-server	8.4p1-150300.3.22.1	D/L and verification by the TOE
11	SW (rpm package)	kernel-default (for intel)	5.14.21-150400.24.81.1	D/L and verification by the TOE
12	SW (rpm package)	ucode-intel	20230808-150200.27.1	D/L and verification by the TOE
13	SW (rpm package)	audit-audispd-plugin	3.0.6-150400.4.6.1	D/L and verification by the TOE
14	SW (rpm package)	yast2-online-update	4.4.5-150400.3.6.1	D/L and verification by the TOE

No	Type	Identifier	Release	Form of Delivery
15	SW (rpm package)	yast2-online-update-configuration	4.4.1-150400.3.10.1	D/L and verification by the TOE
16	SW (rpm package)	firewalld	20230808-150200.27.1	D/L and verification by the 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 the Evaluated Configuration Guide [10].

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, User data protection, Identification and Authentication, Security Management, Protection of the TSF, TOE Access, Trusted Path/Channel.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

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

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

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

The SLES evaluation covers a potentially distributed network of systems running the evaluated versions and configurations of SLES as well as other peer systems operating within the same management domain. The hardware platforms selected for the evaluation

consist of machines which are available when the evaluation has completed and to remain available for a substantial period of time afterwards.

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

The hardware, the BIOS/UEFI 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 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.

6. Documentation

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

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

7. IT Product Testing

The evaluator performed all the tests defined in the General Purpose Operating System Protection Profile (PP) [8] and the SSH Functional Package (FP) [9] which are approximately 100 tests. For the test requirements on crypto primitives and RNG, the ACVP tests were performed on all applicable cryptographic algorithms.

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

The evaluator tests are partly manual tests and partly automated.

The evaluator verified the correct setup of the test systems according to the documentation in the Evaluated Configuration Guide (EVG) [10] and the ETP. The evaluator tested on the hardware setups named in Chapter 8 below. All tests were performed on all hardware platforms.

7.1. Evaluator Testing

Two types of tests were performed: independent testing as defined by the Protection Profile [8] and the Functional Package [9] as well as CAVS algorithm testing.

Independent testing 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:

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

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

No deviation from the expected results have been encountered.

7.2. Evaluator Penetration Testing

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

Linux standard tools (dbus-send and basic shell commands) have been used as part of the testing.

In summary, the following aspects were subject to testing:

- Check for DOWNFALL processor vulnerability mitigation
- Potentially inappropriately controlled DBus services
- Undocumented security-relevant programs
- Potentially inappropriate access control to configuration files
- Unexpected network interfaces
- 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 as also listed in the Evaluated Configuration Guide [10], section 1.3.1 and the Security Target [6], section 1.5.1:

- x86_64 Intel Cascade Lake processors on Delta D20x-M1-PC-32-8-96GB-1TB-2x1G
- x86_64 AMD EPYC 1st Generation processors on Gigabyte R181-Z90
- ARMv8.2-A processors on Gigabyte R181-T90
- IBM Power 10 processors on IBM Power10 9080-HEX
- IBM z15 processors on IBM Z System z15

The installation of the TOE must be carried out as described in Evaluated Configuration Guide [10], 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 claimed in the Security Target [6], chapter 6 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 [8]

  Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP [9]

Technical Decisions listed in Chapter 2.1.1 and 2.1.2 in the Security Target [6]

- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 extended
  ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_INT.1, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' 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

ACVP	Automated Cryptographic Validation Protocol
ASLR	Address Space Layout Randomization
AIS	Application Notes and Interpretations of the Scheme
BIOS	Basic Input/Output System
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
CAVS	Cryptographic Algorithm Validation Program
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETP	Evaluator Test Plan
ETR	Evaluation Technical Report
EVG	Evaluated Configuration Guide
FP	Functional Package
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
ISO	International Organization for Standardization
PP	Protection Profile
RNG	Random Number Generator
RPM	Red Hat Package Management
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
SSH	Secure Shell Protocol

ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEFI	Unified Extensible Firmware Interface

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.

ISO Image - File system image typically containing ISO 9660 or URF file systems

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-1213-2023, Version 1.4, 2023-12-05, SUSE Linux Enterprise Server 15 SP4, SUSE LLC

[7] Evaluation Technical Report, Version 8, 2023-12-05, 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] Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021, CCEVS-VR-PP-0075, NIAP

[10] Common Criteria Evaluated Configuration Guide for SUSE LINUX Enterprise Server 15 SP4 (NIAP), Version 4.0, 2023-11-10, atsec information security GmbH and SUSE LLC

[11] Configuration list for the TOE, 2023-11-03, Master Configuration List, SUSE LLC (confidential document)

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- 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-1213-2023

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-PKCS1-v1.5 using SHA-2 (rsa-sha2-256 or rsa-sha2-512)	[RFC8017],PKCS#1 v2.2sec.8.-2(RSA) [FIPS180-4] (SHA) [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7(SSHAUTH) for user authentication	Modulus length: 2048, 3072 and 4096	Yes	Pubkeys are exchanged trustworthily out of band, e.g. checkingfingerprints. Authenticity is not part of the TOE.
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{256,3-84,521}r1 [SEC2] [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	plength= 256, 384, 521 depends on selected curve	Yes	
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 authentication is aborted the counter for failed logins is increased and remains as is for the next login.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
4	Key agreement (key exchange)	DH with diffie-hellman-group-exchange-sha256 and 512 (for RSA)	[RFC4253](SSH-TRANS) supported by [RFC4419] and [RFC8268](DH-Group Exchange) [FIPS-180-4] (SHA)	plength= 2K, 3K, 4K, etc.	Yes	As of /etc/ssh/m-oduli
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}r 1 [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 GCM mode (aes128-cbc, aes256-cbc) (aes128-gcm, aes256-gcm);	[FIPS197] (AES), [SP800-38A] (CBC), [RFC 4253] (SSH-TRANS using AES with CBC mode), [RFC8268] (SSH-2 using AES with GCM mode)	|k|=128, 256	Yes	
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-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-	[RFC5647]	|k|=128, 256	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		gcm@openssh.com, aes256-gcm@openssh.com)				
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. [RFC8332]	n/a	n/a	Using FCS_RBG_EXT.1
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	Modular exponentiation DH key exchange with key size: 2048, 4096, 8192 bits	[RFC4253] chapter 8 [RFC8268] sec. 5.6.1.1.4	n/a	n/a	Using FCS_RBG_EXT.1
13		ECDSA key generation based on the NIST curves: P-256, P-384, and P-521	[SP800-56A-Rev3], sec. 5.6.1.2.2 [RFC4253] [RFC4306]	n/a	n/a	
14	Trusted channel	FTP_ITC_EXT.1 ST [6], sec. 7.2.8.1 for SSH v2	Cf. all lines for SSH above	See above	n/a	

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	Key derivation with authentication (access control, protection / recovery mode)	Password based key derivation using PBKDF2 with PRF HMAC using SHA-256, SHA-384, SHA-512	[SP800-132] [RFC2898] (PBKDF2) [FIPS198-1](HMAC) [FIPS180-4](SHA)	Guessing prob. 2^{-20} Salt 32 byte (LUKS_SALTSIZE) iteration count 1000 ms	Yes	
2	Confidentiality	AES in XTS mode	[FIPS197]	|k|= 2*128,	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
	(bulk data & key access / key wrapping)	IV-handling mechanism: XTS-plain64 XTS-benbi	[SP800-38E] (XTS)	2*192, 2*256		

Table 4: TOE cryptographic functionality for LUKS/dm-crypt

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-256 HMAC-SHA-384 HMAC-SHA-512 AES GMAC used by GCM	[RFC4868] [FIPS180-4] (SHA) [FIPS198-1] (HMAC) [SP800-38D] (GCM / GMAC)	Key length equal to digest	Yes	
3	Key Agreement	DH with PQG: FFDHE2048 / 3072 / 4096 / 6144 / 8192 ECDH with curves NIST P-256, NIST P- 384, NIST P-521	[RFC7919], [SP800-56A-rev3]	Keys size as defined by PQG parameters / curves	n/a	
4	IV / Key derivation	PRF SHA-2 with hash type chosen by TLS cipher suite	[RFC5996] [FIPS180-4] [FIPS198-1]	Depending on chosen cipher, compliant to [RFC5246]	Yes	
5	Peer authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-2	[RFC 5246] [FIPS 186-4] [FIPS 180-4] [RFC8017], (PKCS#1v2.2) Sec. 8 (RSA)	Modulus >= 2048 bits Keys size as defined by curves	Yes	
		RSA signature generation and verification RSASSA-PSS using SHA-2				
		ECDSA with	[RFC5246] Sec1-v2			

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		signature generation and verification using SHA-2 with NIST P-256, P-384, P-521	(ECDSA) ([SEC2]) [FIPS180-4] (SHA)			
6	Key generation for authentication	ECDSA using NIST P-256, P-384, P-521	[FIPS186-4], B.4	Modulus >= 2048 bits Keys size as defined by curves	Yes	
		RSA with 3072, 4096 bits 4 rounds of Miller-Rabin	[FIPS186-4], 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-rev3] section 5.6.1.1.4 [RFC5246]	Keys size as defined by PQG parameters	n/a	
		ECDSA with 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_EXT.1 ST [6], Sec. 7.2.8.1 for TLS v1.2	Cf. all lines for TLS above	-	n/a	
9	Random number generator	CTR DRBG with AES- 256, with DF, without PR	[SP800-90A-Rev1]	-	n/a	

Table 5: TOE cryptographic functionality for TLS

References for table 3 to 5:

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

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

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

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

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

RFC2104 **HMAC: Keyed-Hashing for Message Authentication**

	Author(s)	H. Krawczyk, M. Bellare, R. Canetti
	Date	1997-02-01
	Location	http://www.ietf.org/rfc/rfc2104.txt
RFC2898	**PKCS #5: Password-Based Cryptography Specification Version 2.0**	
	Author(s)	B. Kaliski
	Date	2000-09-01
	Location	http://www.ietf.org/rfc/rfc2898.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
RFC4251	**The Secure Shell (SSH) Protocol Architecture**	
	Author(s)	T. Ylonen, C. Lonvick
	Date	2006-01-01
	Location	http://www.ietf.org/rfc/rfc4251.txt
RFC4252	**The Secure Shell (SSH) Authentication Protocol**	
	Author(s)	T. Ylonen, C. Lonvick
	Date	2006-01-01
	Location	http://www.ietf.org/rfc/rfc4252.txt
RFC4253	**The Secure Shell (SSH) Transport Layer Protocol**	
	Author(s)	T. Ylonen, C. Lonvick
	Date	2006-01-01
	Location	http://www.ietf.org/rfc/rfc4253.txt
RFC4306	**Internet Key Exchange (IKEv2) Protocol**	
	Author(s)	C. Kaufman
	Date	2005-12-01
	Location	http://www.ietf.org/rfc/rfc4306.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
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
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
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
RFC7919	**Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)**	
	Author(s)	D. Gillmor
	Date	2016-08-01
	Location	http://www.ietf.org/rfc/rfc7919.txt
RFC8268	**More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)**	
	Author(s)	M. Baushke
	Date	2017-12-01
	Location	http://www.ietf.org/rfc/rfc8268.txt
RFC8332	**Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol**	
	Author(s)	D. Bider
	Date	2018-03-01
	Location	http://www.ietf.org/rfc/rfc8332.txt
SEC2	**Recommended Elliptic Curve Domain Parameters**	
	Date	2000
	Location	http://www.secg.org
SP800-38A	**Recommendation for Block Cipher Modes of Operation: Methods and Techniques**	
	Date	2001-12-01
	Location	https://csrc.nist.gov/pubs/sp/800/38/a/final
SP800-38D	**Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**	
	Date	2007-11-28
	Location	https://csrc.nist.gov/pubs/sp/800/38/d/final
SP800-38E	**Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices**	
	Date	2010-01-18
	Location	https://csrc.nist.gov/pubs/sp/800/38/e/final
SP800-56A-Rev3	**Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography**	
	Date	2018-04-16
	Location	https://csrc.nist.gov/pubs/sp/800/56/a/r3/final

SP800-90A-Rev1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators**	
	Date	2015-06-24
	Location	https://csrc.nist.gov/pubs/sp/800/90/a/r1/final
SP800-132	**Recommendation for Password-Based Key Derivation: Part 1: Storage Applications**	
	Date	2010-12-22
	Location	https://csrc.nist.gov/pubs/sp/800/132/final

Note: End of report