Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1165-2022

for

IBM AIX 7.2.5

Service Pack 3 (SP3) Standard Edition (SE)

from

IBM Corporation

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1165-2022 (*)

Operating System

IBM AIX 7.2.5
Service Pack 3 (SP3) Standard Edition (SE)

from	IBM Corporation
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 ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1

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, 8 July 2022

For the Federal Office for Information Security

Matthias Intemann
Head of Branch

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

[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.

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

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

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 IBM AIX 7.2.5, Service Pack 3 (SP3) Standard Edition (SE) has undergone the certification procedure at BSI.

The evaluation of the product IBM AIX 7.2.5, Service Pack 3 (SP3) Standard Edition (SE) was conducted by atsec information security GmbH. The evaluation was completed on 29 June 2022. 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: IBM Corporation.

The product was developed by: IBM Corporation.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 July 2022 is valid until 7 July 2027. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

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 IBM AIX 7.2.5, Service Pack 3 (SP3) Standard Edition (SE) 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] IBM Corporation
11400 Burnet Road
Austin, TX 78758
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 a general purpose, multi-user, multi-tasking operating system. It is compliant with major international standards for UNIX systems, such as the Portable Operating System Interface (POSIX) standards, X/Open Portability Guide (XPG) 4, and Spec 1170. It provides a platform for a variety of applications in the governmental and commercial environment. AIX is available on a broad range of computer systems from IBM, ranging from departmental servers to multi-processor enterprise servers, and is capable of running in a Logical Partition (LPAR) environment.

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 [8]. 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
Auditing	The TOE contains an audit mechanism that generates local audit records and stores them in local audit files.
Cryptographic Support	The TOE includes an SSH client and server using OpenSSH 8.1p1. The TOE also includes TLS client support using the 32-bit OpenSSL that resides in user space. The TOE supports two trusted update mechanisms: cumulative updates and interim fixes (ifixes) which use Java and OpenSSL to assert trust. The TOE includes an Encrypted File System (EFS) feature for encrypting sensitive data stored on non-volatile storage. In addition, the TOE's boot integrity code uses the CLiC cryptographic module in kernel space. The TOE also performs key destruction of private keys and key material in volatile and non-volatile memory under certain conditions.
User Data Protection	The TOE's Journaled File System version 2 (JFS2) supports the standard UNIX permission bit access control mechanism to protect both TSF and user data in named file system objects such as files and directories.
Identification and authentication	The TOE supports authentication failure handling. The TOE supports multiple authentication mechanisms. The TOE's TLS client includes support for certificate-based authentication of a TLS connection
Security management	The TOE supports management of its security features by administrators. These management features include the

TOE Security Functionality	Addressed issue
	following: - Session timeout - Auditing: - Audit storage capacity configuration - Audit event/rule configuration - Password composition configuration - Firewall configuration Users can modify their session timeout values.
Protection of the TSF	The TOE uses the access control mechanism to prohibit unprivileged users from modifying TSF functions such as the kernel, device drivers, security audit logs, etc. It also prohibits unprivileged users from reading security-relevant data such as security audit logs and system-wide credential repositories. The TOE performs address space layout randomization (ASLR) for all applications unless the application is marked as an exception to ASLR. An administrator can selectively except applications from ASLR. The TOE implements a Stack Execution Disable (SED) protection mechanism to aid in stopping stack buffer overflow attacks. This mechanism prevents processes from executing code residing on the process' stack. The TOE uses digital signatures to validate its bootchain as the TOE boots (a.k.a. boot integrity). The validation includes the bootloader, kernel, device drivers, and kernel extensions. The TOE performs digital signature validation of both OS updates and application updates (a.k.a. trusted update). This mechanism allows an administrator to validate the signatures of the updates prior to installing them. The TOE supports two trusted update mechanisms: - Cumulative updates - Interim fixes (ifixes) The TOE prevents allocation of memory regions with both write and execute permissions in the code, data, heap, and stack segments.
TOE Access	The TOE displays an administrator-configurable advisory warning message before a user session is established.
Trusted path/channel	The TOE supports a TLS client protocol implementation via OpenSSL that allows applications to connect to TLS servers. The TOE supports a general purpose OpenSSH client allowing users to connect to other remote SSH servers via a secure connection.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

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:

IBM AIX 7.2.5, Service Pack 3 (SP3) Standard Edition (SE)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	ISO	AIX_v7.2_Install_7200-05-03-2136_flash_092021_LCD8236411.iso (SHA256: d63c2844baec2f1a21d2caed6925c85a87f14abdd22c54324cf63f714197131f)	7.2.5	D/L
2	DOC	AIX 7.2 Technology Level 5 Service Pack 3 Common Criteria Administration Guidance Version 1.3 (SHA256: 2a5c9a1a4a2993463d8e8cf736add9b25fcd0648271139891c8f4e0a01dfe8ee)	1.3	D/L
3	DOC	AIX 7.2 Reference Documentation (SHA256: 5a55b80a6e9c356eb939a9a01b95d1263c6cb3b3e836923a22d299517b3098a3)	N/A	D/L
4	TAR	CCEMGR_fix (SHA256: 21917e86ea568d2b28dc87c4cf2b5e6727567cd51d6249b12dfa66faa415947f)	N/A	D/L
5	TAR	CCECCSUMA1_fix (SHA256: 7ab9a64cd98d0b8160e6fc0b67b0cd72c9779315b9ad293659e9a98dfa5c33e8)	N/A	D/L
6	TAR	InstTU_fix (SHA256: a2606ac587237cdc60ab30ebc6793e94c607f69f8bdf0d4910b4d9749d79d414)	N/A	D/L
7	TAR	TD0325_fix	N/A	D/L

No	Type	Identifier	Release	Form of Delivery
		(SHA256: cbbdff7aabec93b022872a4e57c9cf683ac806b1e0bcbf0dbbc1fa4fd9f32a5b)		
8	TAR	efs_fix (SHA256: 206fa67aae93f1a1df78b287e50a3d972092998a80b5320b1dfe3e4c00651cf3)	N/A	D/L
9	TAR	lscore_fix (SHA256: c4f97465829e8a25cccf326005738362663 5b5922f181a9450e6a5fbbf3558b9)	N/A	D/L
10	TAR	mount_fix (SHA256: 438f2e0d1bddedbb4983e962538664b8f0c14899233b859c9dd2e66228484835)	N/A	D/L
11	TAR	openssh_fix14 (SHA256: 23a32151be35c6322d80d4a3633effff92ed3bab8b45cc21f3494c5d92cf7678)	N/A	D/L
12	TAR	audit_fix (SHA256: 0c2ef6fcc0f743e0a1a0ab71a9451f1ca592c663eb434c6af5219bea98cd1aeb)	N/A	D/L
13	TAR	kernel_fix3 (SHA256: b217d346b5a6312ec15911ca9cbf64a5da098edbf8b47644273d71736c12de18)	N/A	D/L
14	TAR	java_feb2022_fix (SHA256: 68f682d919024ab8eb1db5ab4fdcd1037709605424a55df5b7980baa9ff003e7)	N/A	D/L

Table 2: Deliverables of the TOE

The TOE is distributed by download only. The ISO image for the initial TOE installation as well as the download of the ifixes required for the evaluated configuration, are to be downloaded from the IBM webpage over HTTPS.

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 and 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 upon a trustworthy computing platform for its execution.
- The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
- 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 3.2.1.

5. Architectural Information

AIX is a general purpose, multi-user, multi-tasking Unix based operating system.The TOE Security Functionality (TSF) consist of functions of AIX 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 TOE supports standard networking applications and protocols, including applications allowing access of the TOE via cryptographically protected communication channels, such as SSH and TLS. System administration tools include the standard command line tools. A user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE provides the following security functionality:

Auditing

The TOE contains an audit mechanism that generates local audit records and stores them in local audit files.

Cryptographic Support

The TOE includes an SSH client and server using OpenSSH 8.1p1. The TOE also includes TLS client support using the 32-bit OpenSSL that resides in user space. The TOE supports two trusted update mechanisms: cumulative updates and interim fixes (ifixes) which use IBM Java 8.6.30 TLS 1.2 client implementation and OpenSSL to assert trust. The TOE includes an Encrypted File System (EFS) feature for encrypting sensitive data stored on non-volatile storage. In addition, the TOE's boot integrity code uses the CLiC cryptographic module in kernel space. The TOE also performs key destruction of private keys and key material in volatile and non-volatile memory under certain conditions.

User Data Protection

The TOE's Journaled File System version 2 (JFS2) supports the standard UNIX permission bit access control mechanism to protect both TSF and user data in named file system objects such as files and directories.

Identification and authentication

The TOE supports authentication failure handling. Also, the TOE supports multiple authentication mechanisms, specifically username/password-based and key-based authentication. The SSH server supports remote administration using username/password-based and key-based authentication. The SSH client also supports both username/password-based and key-based authentication. The TOE's TLS client includes support for certificate-based authentication of a TLS connection.

Security management

The TOE supports management of its security features by administrators. These features include the following: session timeout, auditing (audit storage capacity configuration and audit event/rule configuration), password composition configuration and firewall configuration. Users can modify their session timeout values.

Protection of the TSF

The TOE uses the access control mechanism to prohibit unprivileged users from modifying TSF functions such as the kernel, device drivers, security audit logs, etc. It also prohibits unprivileged users from reading security-relevant data such as security audit logs and system-wide redential repositories. The TOE performs address space layout randomization (ASLR) for all applications unless the application is marked as an exception to ASLR. The TOE implements a Stack Execution Disable (SED) protection mechanism to aid in stopping stack buffer overflow attacks. This mechanism prevents processes from executing code residing on the process' stack.

The TOE uses digital signatures to validate its bootchain as the TOE boots (a.k.a. boot integrity). The TOE performs digital signature validation of both OS updates and application updates (a.k.a. trusted update). This mechanism allows an administrator to validate the signatures of the updates prior to installing them.

The TOE supports two trusted update mechanisms.

- Cumulative updates
- Interim fixes (ifixes)

Cumulative updates, such as technology level updates and service packs, are provided at scheduled times throughout each year. Ifixes are provided in between cumulative updates making critical fixes available as soon as possible. Both update mechanisms can include security updates. The TOE prevents allocation of memory regions with both write and execute permissions in the code, data, heap, and stack segments.

TOE Access

The TOE displays an administrator-configurable advisory warning message before a user session is established.

Trusted path/channel

The TOE supports a TLS client protocol implementation via OpenSSL that allows applications to connect to TLS servers. The suma command uses the IBM Java TLS client implementation to connect to the IBM fix server over HTTPS. The ifix commands use the OpenSSL TLS client implementation to connect to the IBM fix server over HTTPS. The TOE supports a general purpose OpenSSH client allowing users to connect to other remote SSH servers via a secure connection. It also supports inbound remote administration connections over SSH using OpenSSH.

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

7.1. Evaluator Independent Testing

Testing effort

The evaluator performed all the tests defined in the OSPP and SSH-EP, which are around 100 tests. For the test requirements on crypto primitives and RNG, the ACVP tests were performed on all applicable cryptographic algorithms.

Test approach

The evaluator followed the test requirements from the PP [8] and EP [11], and constructed the tests. He used the test plan, which explains the test configuration, and links the test requirements (including the complete text specification from the PP [8] and EP [11]), to the actual test procedure.

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

Test configuration

The evaluator verified the correct setup test systems according to the documentation in the Common Criteria Administration Guidance [9] and the test plan.

The evaluator tested setup defined in the Evaluation Technical Report, [7], chapter 3.2:

Hardware:

- IBM Power System E950 rack mounted server with an IBM POWER9 SMT8 core processor and system firmware FW950
- IBM PowerVM Virtual I/O System (VIOS) version 3.1.1

Software:

- IBM AIX Standard Edition, Program Number 5765-G98, VRM1 07.02.05.03
- OpenSSH Client Software
- OpenSSH Server Software
- opensslfips-20.16.102.2103

In addition, the following ifixes (defined also in Table 2) were installed:

- CCEMGR_fix
- CCECCSUMA1_fix
- InstTU_fix
- TD0325_fix
- java_sep2021_fix

- efs_fix
- lscore_fix
- mount_fix
- openssh_fix14

The evaluator notes, that this configuration is considered to be consistent with the one defined in the Security Target [6], chapter 1.5.3.3. After the testing was concluded, the developer, on 2022-03-03, announced three new ifixes, two of which are new and one replaces a previous ifix:

- audit_fix, new ifix.
- kernel_fix3, new ifix.
- java_feb2022_fix, which replaces java_sep2021_fix, which was installed for the evaluator's testing efforts.

The evaluator examined the additional and changed ifixes and determined their changed functionality does neither impact any TSF nor any tested functionality. The evaluator therefore determines, that the application of the ifixes mentioned above do not invalidate the test results obtained.

Test Depth

Two types of tests were performed - independent testing as defined by the OSPP and SSH-EP 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 behavior 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 and and buffer overflow 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 PP [8] and EP [11]. A function of the lab‘s ACVP tool function was used to compare the TOE test vector responses (used in the official CAVP certification) against the responses of a local reference implementation under control of the lab. All of the test results could be validated by the lab using the reference implementation.

Verdict: No deviation from the expected results have been encountered.

7.2. Evaluator Penetration Testing

The evaluator's search for publicly available vulnerability information was performed on multiple occasions, predominately using the general CVE database. The developer's AIX CVE database was also used to confirm findings and obtain more detail via linked AIX support pages. The evaluator examined the operating system system calls (covering general system availability), the various installation methods the TOE provides as well as the TOE's networking profile and configuration.

Verdict: None of the tests were able to penetrate the TOE's TSF with claimed attack potential ‘basic’.

8. Evaluated Configuration

This certification covers the configuration of the TOE specified in the ST [6], section 1.5.3.3 which is also defined in the evaluated Common Criteria Administration Guidance [9], section 3.

The evaluated hardware platform for the TOE is the one specified in the Securirty Target [6], section 1.4: IBM Power System E950 rack mounted server with an IBM POWER9 SMT8 core processor, VIOS Version 3.1.1 , System Firmware FW950.

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 and AIS 31 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.

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
  ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 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*' of the following table 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 and Threats 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.

In addition, the following aspects need to be fulfilled when using the TOE:

- As defined in the Security Target [6]: The ICC-cryptographic module's RNG shall only be used with the TOE's suma command and for no other purposes.

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
CAVP	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
EAL	Evaluation Assurance Level
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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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.

Exact Conformance - a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the requirements in the Security Requirements section of the PP, and potentially requirements from Appendices of the PP. While iteration is allowed, no additional requirements (from the CC parts 2 or 3) are allowed to be included in the ST. Further, no requirements in the Security Requirements section of the PP are allowed to be omitted.

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-1165-2022, Version 1.3, 2022-06-21, IBM AIX 7.2 Technology Level 5 Service Pack 3 Standard Edition Operating System Security Target, IBM Corporation

[7] Evaluation Technical Report, Version 7, 2022-06-28, 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] Guidance Documentation for the TOE, Version 1.3, 2022-04-04 IBM AIX 7.2 Technology Level 5 Service Pack 3 Common Criteria Administration Guidance

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[10] Configuration List for the TOE, Version 0.9, 2022-06-20, IBM AIX Version 7.2 Technology Level 5 (TL5) Service Pack 3 (SP3) Life Cycle, (confidental document)

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

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-1165-2022

Overview and rating of cryptographic functionalities implemented in the TOE

1.1. Boot Integrity

Boot Integrity is achieved with CliC.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Integrity verification	RSA PKCS1 v1.5 signature verification with SHA-256	FIPS 186-4	Modulus size 2048 bits	✓	-

Table 3: TOE cryptographic functionality for Boot Integrity

1.2. Encrypted File System (EFS)

Encrypted File System (EFS) cryptographic functions are provided by CliC.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Confidentiality	Cipher: AES Modes: CBC	FIPS 197 SP800-38A	128, 256	✓	-
2	Key generation to obtain per-user KEK	RSA 16 rounds of Miller-Rabin	FIPS 186-4, B.3.3 and C.3 for Miller Rabin primality tests.	Modulus size 2048 bits, 4096 bits	✓	-
3	Key wrapping	RSA	FIPS 186-4	Modulus size 2048 bits, 4096 bits	✓	-
4	Random number generation	Hash DRBG with SHA-512 core, no PR	SP800-90A-Rev1 FIPS 180-4	-	-	-

Table 4: TOE cryptographic functionality for Encrypted File System (EFS)

1.3. SSH

SSH cryptographic functions are provided by OpenSSL.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Confidentiality	Cipher: AES Modes: aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm, aes256-gcm	FIPS 197 (AES) SP800-38A (CBC, CTR) SP800-38D (GCM) RFC4344 RFC 4253 (SSH-TRANS)	128, 256	✓	-
2	Integrity and Authenticity	HMAC SHA-1 (hmac-sha1) HMAC-SHA-256 (hmac-sha2-256) HMAC-SHA-512 (hmac-sha2-512)	FIPS180-4 (SHA) RFC2104, FIPS198-1 (HMAC) RFC4251/ RFC4253 (SSH HMAC support) RFC6668 (SHA-2 support for SSH)	Key length equal to digest length	✓	-
3	Key establishment: key agreement	ECDH with: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521	RFC4253 (SSH-TRANS) RFC5656 (ECDH for SSH) Sec1-v2	Depending on the curve	✓	-
4	IV/Key derivation	PRF SHA-1 / SHA-2 with hash type defined by selected ECDH key agreement mechanism outlined above	RFC4253 FIPS 180-4	Depending on chosen cipher, compliant to RFC4253	✓	-
5	Authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-256 or SHA-512 (ssh-rsa-256, ssh-rsa-512)	FIPS 186-4 RFC3447, (PKCS#1v2.1) Sec. 8.2 (RSA) RFC4253, Sec. 6.6 (SSH-TRANS) for host authentication RFC4252, Sec. 7 (SSH-	2048 3072 4096	✓	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
			USERAUTH) for user authentication method: “publickey”			
		ECDSA with signature generation and verification using SHA-2 and NIST P-256, P-384, P-521 (ecdsa-sha2-nistp256, ecdsa-sha2-nistp384)	FIPS 186-4 RFC4253, Sec. 6.6 (SSH-TRANS) for host authentication RFC4252, Sec. 7 (SSH-USERAUTH) for user authentication method: “publickey” RFC 5656 (ECDSA for SSH) Sec1-v2 (ECDSA) FIPS180-4 (SHA)	Keys size as defined by curves	✓	-
6	Key generation for authentication	RSA 5 (2048 bits and lower), 4 (larger key sizes) rounds of Miller-Rabin	FIPS 186-4, B.3.3 and C.3 for Miller Rabin primality tests.	2048 3072 4096	✓	-
		ECDSA with NIST P-256, P-384	FIPS 186-4, B.4	Keys size as defined by curve	✓	-
7	Key Generation for ECDH	ECDSA with NIST P-256, P-384, P-521	SP800-56A rev. 3 section 5.6.1.2.2 RFC4253	Keys size as defined by curves	✓	-
8	Trusted Channel	FTP_ITC_EXT.1, ST	See list above	-	-	Only SSHv2 (RFC4253) is supported in the evaluated configuration.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
9	Random number generation	CTR DRBG with AES-256, with DF, without PR	SP800-90A-Rev1	-	-	-

Table 5: TOE cryptographic functionality for SSH

1.4. TLS (OpenSSL)

TLS protocol including the cryptographic primitives are provided by OpenSSL.

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, RFC5289 GCM: RFC5288, RFC5289 FIPS 197 (AES) SP800-38A (CBC) SP800-38D (GCM)	128, 256	✓	-
2	Integrity and authenticity	HMAC SHA-1 HMAC-SHA-256 HMAC-SHA-384 AES GMAC used by GCM	RFC5246 FIPS 180-4 (SHA) FIPS 198 (HMAC) SP800-38D (GCM / GMAC)	Key length equal to digest length	✓	-
3	Key Agreement	ECDH with NIST P-256, NIST P-384, NIST P-521	RFC5246 SP800-56A rev. 3	Keys size as defined by curves	✓	-
4	Key Transport	RSAES-PKCS1-v1.5 Encryption/Decryption	RF5246 FIPS 186-4	Modulus 2048 bits, 3072 bits, 4096 bits	✓	-
5	IV / Key derivation (TLSv1.0/1.1 v1.2 handshake)	PRF SHA-1/MD5 and SHA-2 with hash type chosen by TLS cipher suite	RFC1321 RFC5246 FIPS 180-4 FIPS 198	Depending on chosen cipher, compliant to RFC5246	✓	-
6	Peer authentication	RSA signature generation and verification RSASSA-	RFC 5246 FIPS 186-4 FIPS 180-4	Modulus 2048 bits, 3072 bits, 4096 bits	✓	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		PKCS1-v1.5 using SHA-1 and SHA-2	RFC3447, (PKCS#1v2.1) Sec. 8 (RSA)	Keys size as defined by curves		
		RSA signature generation and 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	FIPS 186-4 (ECDSA) FIPS180-4 (SHA)			
7	Key generation for authentication	ECDSA using NIST P-256, P-384, P-521	FIPS 186-4, B.4	Modulus 2048 bits, 3072 bits, 4096 bits Keys size as defined by curves	✓	-
		RSA 5 (2048 bits and lower), 4 (larger key sizes) rounds of Miller-Rabin	FIPS 186-4, B.3.3 and C.3 for Miller Rabin primality tests			
8	Key generation for ECDH	ECDSA with NIST P-256, P-384, P-521	SP800-56A rev. 3 section 5.6.1.2.2 RFC4306	Keys size as defined by curves	✓	-
9	Trusted Channel	FTP_ITC_EXT.1, ST TLS	See listed above	-	-	-
10	Random number generation	CTR DRBG with AES-256, without DF, without PR	SP800-90A-Rev1	-	-	-

Table 6: TOE cryptographic functionality for TLS (OpenSSL)

1.5. TLS (ICC)

The TLS protocol implementation used by the suma command including the cryptographic primitives are provided by the ICC librabry.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Confidentiality	Cipher: AES Modes: GCM	GCM: RFC5288, RFC5289 FIPS 197 (AES) SP800-38D (GCM)	128, 256	✓	-
2	Integrity and authenticity	HMAC SHA-1 HMAC-SHA-256 HMAC-SHA-384 AES GMAC used by GCM	RFC5246 FIPS 180-4 (SHA) FIPS 198 (HMAC) SP800-38D (GCM / GMAC)	Key length equal to digest length	✓	-
3	Key Transport	RSAES-PKCS1-v1.5 Encryption/Decryption	RF5246 FIPS 186-4	Modulus 2048 bits, 3072 bits, 4096 bits	✓	-
4	IV / Key derivation (TLSv1.0/1.1 v1.2 handshake)	PRF SHA-1/MD5 and SHA-2 with hash type chosen by TLS cipher suite	RFC1321 RFC5246 FIPS 180-4 FIPS 198	Depending on chosen cipher, compliant to RFC5246	✓	-
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, 3072 bits, 4096 bits Keys size as defined by curves	✓	-
		RSA signature generation and verification RSASSA-PSS using SHA-1 and SHA-2				
6	Trusted Channel	FTP_ITC_EXT.1, ST TLS	See listed above	-	-	-
7	Random number generation	Hash DRBG with AES-256, without DF, without PR	SP800-90A-Rev1	-	-	-

Table 7: TOE cryptographic functionality for TLS (ICC)

1.6. Trusted Update

The Trusted Update functionality uses OpenSSL to access cryptographic primitives.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Integrity verification	RSA PKCS1 v1.5 signature verification with SHA-1, SHA-256, SHA-384, SHA-512	FIPS 186-4	Modulus size 2048 bits, 3072 bits, 4096 bits	✓	-

Table 8: TOE cryptographic functionality for Trusted Update

References for Table 3 to 8:

FIPS140-2 Security Requirements for Cryptographic Modules
Date 2002-12-03
Location https://csrc.nist.gov/publications/detail/fips/140/2/final

FIPS140-3 Security Requirements for Cryptographic Modules
Date 2019-03-22
Location https://csrc.nist.gov/publications/detail/fips/140/3/final

RFC4251 The Secure Shell (SSH) Protocol Architecture
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01

RFC4252 The Secure Shell (SSH) Authentication Protocol
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01

RFC4253 The Secure Shell (SSH) Transport Layer Protocol
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01

RFC4254 The Secure Shell (SSH) Connection Protocol
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4254.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

RFC0793 Transmission Control Protocol

Author(s) J. Postel

Date 1981-09-01

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

RFC5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

Author(s) E. Rescorla

Date 2008-08-01

Location http://www.ietf.org/rfc/rfc5289.txt

RFC5647 AES Galois Counter Mode for the Secure Shell Transport Layer Protocol

Author(s) K. Igoe, J. Solinas

Date 2009-08-01

Location http://www.ietf.org/rfc/rfc5647.txt

RFC5656 Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer

Author(s) D. Stebila, J. Green

Date 2009-12-01

Location http://www.ietf.org/rfc/rfc5656.txt

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