Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1223-2025

for

Fabric OS, Version 9.1.1b8

from

Brocade Communications Systems 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-1223-2025 (*)

Network Device

Fabric OS, Version 9.1.1b8

from	Brocade Communications Systems LLC
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.2
valid until:	30 September 2030

SOGIS
Recognition Agreement

Common Criteria

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

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

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

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

Common Criteria
Recognition Arrangement

Bonn, 1 October 2025

For the Federal Office for Information Security

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

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

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

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

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

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

This certificate is recognized under CCRA-2014 for all assurance components selected.

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

4. Performance of Evaluation and Certification

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

The product Fabric OS, Version 9.1.1b8 has undergone the certification procedure at BSI.

The evaluation of the product Fabric OS, Version 9.1.1b8 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 11 September 2025. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Brocade Communications Systems LLC.

The product was developed by: Brocade Communications Systems 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 1 October 2025 is valid until 30 September 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

[5] Information Technology Security Evaluation Facility

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

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

6. Publication

The product Fabric OS, Version 9.1.1b8 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] Brocade Communications Systems LLC
1320 Ridder Park Drive
San Jose 95131
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 the Brocade Communications Systems LLC Fabric OS, Version 9.1.1b8 which is running on specific Brocade Directors and Switches hardware appliances from generation 6 and 7. The TOE is configured as instructed by the preparatory documentation as in table 2 which are provided by Brocade Communications Systems LLC. Brocade Communications Systems LLC Fabric OS, Version 9.1.1b8 is a software solution utilizing hardware appliances that implement what is called a 'Storage Area Network' or 'SAN'. SANs provide physical connections between servers that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment. The TOE provides the following major security features:

- auditing of user activity,
- identification and authentication of users,
- management based upon user roles,
- a SAN access policy,
- restrictions upon TOE access,
- encryption supporting communication with network peers, and
- encryption supporting administrative trusted path.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2 augmented by ALC_FLR.2.

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
Security audit	The TOE generates Audit data. The Audit records include date, time of the event, type, user identity that caused the event. The records are sent to a syslog server in the environment.
User data protection	The TOE provides the ability to restrict block-read and block-write operations to connected storage devices that are initiated by host bus adapters. Host bus adapter can only access storage devices that are members of the same zone.
Identification and authentication	The TOE defines administrative users with user identity, password and role. Role permissions determine the functions that administrators may perform. The TOE authenticates administrative users using either its own authentication mechanism or a RADIUS or LDAP Server. Passwords are chosen by a defined policy.

TOE Security Functionality	Addressed issue
Security management	The TOE provides both serial terminal- and Ethernet network-based management interfaces. Each of these types of interfaces provides equivalent management functionality.
TOE access	An IP Filter policy is a set of rules applied to the IP management interfaces as a packet filtering firewall. The IP Filter policy permits or denies traffic to go through the IP management interfaces according to the policy rules.
Trusted path	The TOE enforces a trusted path between the TOE administrators and the TOE using SSHv2 connections for Ethernet connections from the Administrator terminal to the TOE and configured network peers that are providing syslog, RADIUS or LDAP services.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapters 3.3 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:

Fabric OS, 9.1.1b8

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery	SHA-512 Checksum
1	SW	Brocade Communications Systems LLC Fabric OS Version 9.1.1b8	9.1.1b8	Pre-installed on Brocade Director Blade Models, Director Models, Switch Appliance Models	-
2	DOC	Brocade Fabric OS Common Criteria EAL2 User Guide, 9.1.1b8 [9]	fos-91x-cc-eal2.pdf, August 2025	Password-protected user-id for registered users (customers), web download secured with https	ef7c0b2812bc6e215cadea686b0d646df0aa3d2c721b6036a3a5b0b2e082d9d2532f066d0cde608208450bafe771f98579c90f8d532463968247f29734bfd9da

No	Type	Identifier	Release	Form of Delivery	SHA-512 Checksum
3	DOC	Brocade Fabric OS Administration Guide, 9.1.x [10]	fos-91x-admin.pdf, January 11, 2024	Password-protected user-id for registered users (customers), web download secured with https	a739bcdf3498180cf2f6cc285da5e1d90d0cf2f72c21d3313c0734834f970a6cd43f054fb04f101dbc415a20b46d1ac68518fc6a846db821764a01524250b3b3
4	DOC	Brocade Fabric OS Command Reference Manual, 9.1.x [11]	fos-91x-command.pd, January 11, 2024	Password-protected user-id for registered users (customers), web download secured with https	ce37a90dffe022b4e26064af764d23e420e9a8c51ca92b743a3df673c90f9b32afdb4e90d56140f373015fc570d8b5a65623406921908c2c718a535b1c08053d
5	DOC	Brocade Fabric OS Message Reference Manual, 9.1.x [12]	fos-91x-messageref.pdf, 10 April 2018	Password-protected user-id for registered users (customers), web download secured with https	b787636a1463dbd999d8965f87884ff54ec8bd2f1da81df3c7c3cf2234f6c70c9be7e6180f6f805f158ab9c254775899772f6d77ecdd1b7199ac00cd97d4bcbf

Table 2: Deliverables of the TOE

The certified software, Brocade Communications Systems LLC Fabric OS, Version 9.1.1b8, is certified for the following series and models of Brocade Director and Switch products:

- Generation 6 hardware (Gen6HW)
  - Director Blade[7] Models: FC32-48, FC32-64, CPX6, CR32-4, CR32-8 and SX6
  - Director Models: X6-4, X6-8
  - Switch Appliance Models: 7810, G620 and G630
- Gen 7 hardware (Gen7HW)
  - Director Blade Models: FC32-X7-48, FC64-48, CPX7, CR64-4, CR64-8 and SX6
  - Director Models: X7-4, X7-8
  - Switch Appliance Models: G720 and G730

The software loading process is automated and solely controlled by Brocade's engineers. Brocade Fabric OS images are retrieved by authorized Brocade personnel and are transferred securely to factory sites across private networks. After the hardware is loaded with Fabric OS at the manufacturer´s site, the hardware is packaged and the entire crate is shrink-wrapped afterwards. During all steps confidentiality, authenticity and integrity are ensured by Brocade's engineers, by the private network and at Brocade's manufacturer's site.

For documentation and software downloads, Brocade Partner Network and Brocade Connect sites are given access only to registered partners and end users respectively. Guidance documents in these sites are authenticated using an Okta user-id and password

[7] A blade refers to a purpose-built component that is installed in a Brocade Director.

which are provided only to these registered users. Okta is an ID and password management service that provides both Single-Sign-On and universal-directory services.

The TOE-specific guidance is not delivered together with the downloaded non-TOE product. There is no bundle. In one branch of the path available at the web page the non-TOE can be downloaded, in another branch of the path the CC configuration guide can be downloaded. There is no reference from one to the other. Please note that the Common Criteria EAL2 User Guide document clearly requires not using the non-TOE product with the Common Criteria EAL2 User Guide document.

The download of the guidance is protected by a HTTPS channel with TLSv1.2 and RSA 2048 with sha256 signature.

Brocade performs the delivery directly to end customers or to the OEM/channel partner by respecting the same standards. The transport is performed by trusted C-TPAT[8] certified carriers. Brocade selects its carriers by using a request for proposal (RFP) process, where the transport company has to declare to be CTPAT certified. Brocade verifies CTPAT certification before commencement of operations with that transport company. Every delivery has an identifier from the commercial carrier (e.g., tracking number) and contains a packaging list. Each stock keeping unit (SKU) has a detailed bill of materials with numerous specification documents. This ensures authenticity and integrity and confidentiality.

The shrink-wrapped crate is shipped to Brocade's OEM/channel partner then directly to end customers using commercial carriers. After delivering products to the OEM the responsibility for security needs is transferred from Brocade to the OEM, who will handle the delivery to the end customer.

The end customer can initiate an own commercial carrier transport of the pre-installed TOE from Brocade to its site self-dependent. After leaving the manufacturer´s site the end customer's transport service has to ensure authenticity, integrity and confidentiality of the TOE.

On boot up, the user has to verify and confirm that the approved Brocade Communications Systems LLC Fabric OS, Version 9.1.1b8 is pre-installed using "version" or "firmwareshow" command.

Note 1: As it is unequivocally stated in documentation that the download delivery which is also offered does not lead to a certified version of the TOE.

Note 2: Using the BSI Common Criteria Configuration Guide with a download version of Fabric OS will not lead to a certified version.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE implements a role-based access control policy to control administrative access to the system. In addition, the TOE implements policies pertaining to the following security functional classes:

- Security audit
- User data protection

[8]See the US Customs web site for additional information about the CTPAT (Customs-Trade Partnership Against Terrorism) program (https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism).

- Identification and authentication
- Security management
- TOE access
- Trusted path

Specific details concerning the above mentioned security policies can be found in [6], chapter 7.

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:

Security Objectives for the operational environment defined in Security Target	**Description according to ST**
OE.ADMIN	The environment will ensure that the administrators of the system are trustworthy and qualified personnel with sufficient administration skills.
OE.AUDIT	The environment will provide a Syslog server and a means to present a readable view of the audit data.
OE.AUTH_SVR	The authentication server will offer a password policy that requires password length, password strength and a restriction of failed login attempts that is consistent with the requirements of the Security Target.
OE.PKI	The PKI associated with the trusted root certificates that are installed into the TOE utilize cryptographic algorithms and methods appropriate for the protection of the data processed by the TOE.
OE.NETWORK	The Environment will physically protect network communication to and from the TOE from unauthorized disclosure or modification.
OE.MGMT_NET	The SSHv2 administration workstation, syslog server, and (when utilized) the authentication servers that are connected to the management network are operated in a secure environment.
OE.CONFIG	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
OE.PHYCAL	The TOE, HBA and storage devices will be located within controlled access facilities, which will prevent unauthorized physical access.
OE.HARDWARE	The TOE is assumed to run on models of Brocade Directors and Switches that are listed in section 1.3, [6]. In particular it is assumed that the following functionality is available to the TOE: a) Hardware real time clock b) A trustworthy bootloader

Table 3: Security Objectives for the operational environment

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

5. Architectural Information

The Target of Evaluation (TOE) is Fabric Operating System (Fabric OS), Version 9.1.1b8 running on Brocade Directors and Switches hardware appliances. The Brocade Directors and Switches hardware appliances are available in two form factors: a rack-mount Director Chassis with a variable number of blades, or a self-contained switch appliance device.

This chapter gives an overview of the subsystems of the TOE and the corresponding TSF which were objects of this evaluation.

The security functions of the TOE are enforced by the following two subsystems:

- Runtime Subsystem (supports the TSF “Security audit”)
- Fabric OS Subsystem (supports the TSF “Security audit”, “User data protection”, “Identification and authentication”, “Security management”, “TOE access”, “Trusted path”)

Operating system capabilities of the Fabric OS are executed by the Runtime Subsystem. The Runtime Subsystem provides an execution environment for the Fabric OS subsystem.

The following interactions are provided:

- hardware platform,
- device management capabilities,
- memory management,
- process abstractions,
- process control,
- interprocess communication facilities,
- a file system for information storage,
- an IP protocol stack for use with management networking,
- an IP Filtering capability.

The Fabric OS subsystem provides the following major capabilities:

- Logging functionality
- Crypto Support functionality
- Admin functionality
- AAA functionality
- Remote Access functionality
- SAN functionality

The Logging functionality is responsible for the collection of audit records from other TOE software, the insertion of common fields into audit records (e.g., date/time stamps), the short-term, local storage of audit records, the protection of local audit records, and the transmission of audit records to a remote syslog server.

The Crypto Support Functionality is responsible for the cryptographic operations associated with various network protocols (e.g., SSHv2, TLSv1.2). The Crypto Support Functionality also generates SSH & TLS keys.

All networking performed by the Fabric OS Subsystem occurs over either the management network interface or over a SAN network interface. Each model of the TOE installed has at least one management network port (a Director chassis may have more than one). The number of SAN network interfaces varies by model. These SAN network interfaces are used to connect the Fabric OS Subsystem with HBAs and storage devices.

The SAN functionality implements the Fabric OS Subsystem support for traffic on SAN network interfaces, enforcing zoning rules and ensuring encryption of data as configuration dictates. The SAN functionality also provides fibre channel (FC) protocol support for use over physical FC SAN Data ports. The SAN functionality includes a fixed definition of IP Filters that protect the Fabric OS Subsystem and limit network protocols accepted through network ports that are dedicated to SAN data (e.g. Ethernet SAN Data Ports).

The management network is used exclusively to allow administrators to perform management operations on the Fabric OS subsystem, and to support communication with external syslog, RADIUS and LDAP servers.

Over the management network interface, the Remote Access Functionality provides the network protocol support for the SSH and TLS protocols which protect communication between administrators and the Fabric OS subsystem.

The AAA functionality provides network protocol support for the RADIUS and LDAP protocols. These protocols connect the Fabric OS subsystem with an external authentication server. The Runtime Environment provides a local repository for user identification and authentication material.

Together, the Fabric OS subsystem can utilize either locally defined accounts or accounts defined via LDAP and RADIUS for the identification and authentication of administrators.

The Admin functionality provides a command line interface for the configuration and management of the Fabric OS subsystem over an SSH connection and ensures that all users are identified and authenticated before being allowed to perform operations using the Command Line Interface (CLI). Restrictions based upon administrative roles are enforced upon actions taken through the CLI and supports the management of local user accounts and authentication material.

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. Developer test configuration and test approach

Brocade Fabric OS runs on the complete range of Brocade platforms. In general it is the case that tests for any security-relevant TOE function may be performed on any Brocade hardware platform. None of the security-relevant functions contain behaviour that is unique to a particular platform. The test configuration can be applied to an arbitrary device of a switch appliance equivalence class, switch equivalence class or director equivalence class. The tests were executed on every equivalence class.

For testing purpose the TOE is configured strictly following the referenced guidance documentation [9]. At the end of these steps an evaluated version is installed on an above mentioned equivalence class and can be tested in a freshly installed state providing the security features claimed in the Security Target.

Testing of the TOE security functions is provided by a series of automated and manual tests. These tests demonstrate the security-relevant behaviour of the TOE at the interfaces identified in the Functional Specification document and defined in the High-Level Design documentation. The goal of the tests is to demonstrate that the TOE meets the security functional requirements specified in the Security Target. Using the testing resources is optimized by applying an adaptive, white box testing approach to exploit several properties of the TOE.

Developer Test Case Groups are:

- Enable Security Auditing (FAU_GEN.1): Enable security auditing, through the ‘auditcfg’ command and verify that set security alerts are triggered and reported correctly to the syslog/syslog-ng server.
- Account lockout for non admin accounts; successful and unsuccessful login (FIA_AFL.1, FIA_UAU.5, FIA_UID.2, FTA_TSE.1): This test verifies that an account locks out after a configured number of unsuccessful authentication attempts and remains locked for the configured time period.
- Use of Management Functions, including user / group modifications (FMT_SMF.1, FMT_SMR.1, FMT_MTD.1(1), FMT_MTD.1(2), FIA_ATD.1(1)): This test validates user changes are reflected and admin role permissions supersede that of user roles.
- Authenticate incoming and outgoing SSH user with RSA keys (FCS_CKM.1(1).1, FCS_COP.1(2), FCS_CKM.1(2).1): In this test case, user should get all the credentials, like role, in a successful case using single public/private key pair.
- Key and secret deletion (FCS_CKM.4): This test verifies that certificates can be deleted successfully.
- Basic zoning on different HW (FDP_ACF.1, FDP_ACC.1, FMT_MSA.1, FMT_MSA.3): This test verifies zoning of Brocade switches and validates the restriction of access to storage or initiator ports.
- User class cannot supersede the default admin role (FIA_ATD.1(1) FMT_SMR.1): This test covers that no non-admin defined class may supersede the default admin account for that access right (“O” and “M”). Command permissions are defined as either M for modify, O for observe, or N for No.
- Password Policy Management (FIA_ATD.1(1), FIA_ATD.1(2), FIA_SOS.1): This test verifies the functionality of various password policy parameters in a fabric environment.
- Consistent user deny (FIA_UAU.2, FIA_UID.2): This test verifies that password changes for all user accounts that can access the switch will be denied if account verification is rejected. Additionally verifies that no authentication data is feedbacked to the user while inputting authentication data.
- RADIUS and LDAP authentication (FTA_MCS.1, FIA_UAU.5): This test covers the authentication facility available to firmware by communicating to RADIUS and LDAP servers.
- Cipher configuration with SSH and TLS ciphers (FCS_CKM.1(1).1, FCS_COP.1(1), FCS_COP.1(2), FCS_CKM.2, FTP_ITC.1, FTP_TRP.1): This test verifies that the cipher suites function correctly when editing the ciphers allowed for SSH sessions.

- Maximum number of sessions for each role (FMT_SMR.1, FTA_MCS.1): This test verifies that the total number of SSH sessions that are allowed is limited to 32. The local authentication will limit users according to four sessions per account with the exception of ‘admin’ which is only allowed two sessions.
- IPFILTER robustness (AVA_VAN.2): This test verifies that ports can be opened and closed by changing the active IPFILTER policy.

7.2. Independent Evaluator Tests

The independent testing was partially performed using the developer’s testing environment, partially using the test environment of the evaluation facility. The configuration of the TOE being intended to be covered by the current evaluation was tested.

The TOE was tested in DMZ with a stand-alone test computer and additional workstations. The TOE was running on one machine of each equivalence class and was configured according to chapter 1.4 of the ST [6]. The evaluator has started the TOE and configured it together with the developer. This was done by directly booting up the TOE after the start-up of the machine.

Besides the requirements described in chapter 1.4 of [6] the test environment also needs to fulfil the security objectives for the environment. These security objectives are fulfilled by the following services. The testers starting a SYSLOG server in the test network (OE.AUDIT, OE.MGMT_NET). Only a secure connection (SSH) is used to configure the TOE. The authentication server is installed with username and password (OE.AUTH_SVR). The test environment is located in a secured server room and in a distinct DMZ (OE.NETWORK, OE.PHYCAL, OE.MGMT_NET). The installation instructions are used as outlined in section 1.4.2 of [6] (OE.CONFIG). Tests are executed only with Brocade Directors and Switches that are listed in section 1.2 of [6] (OE.HARDWARE).

These above described components match the needed components described in the guidance documentation [9] to establish the TOE. The TOE environment and the related test equipment for the tests are consistent with the described ones in [6] and [9]: The tests of the TOE are carried out by executing the test environment. There are four standard workstations and six appliances with the TOE installed. In detail there are six appliances, one of each equivalence class with a redundant appliance. The four workstations represent the two Authentication servers, syslog server and a testing workstation. The entire developer test configuration and the test protocols were made available to the evaluator.

Test configuration used for testing:

Hardware:	G620 (Eq Cl1) X6-4(Eq Cl2) X7-4 (Eq Cl3) G730 (Eq Cl4) G630 (Eq Cl5) G720 (Eq Cl6)
Software:	Brocade Communications Systems LLC Fabric OS Version 9.1.1b8
	LDAP (slapd –v on Linux), 2.4.44
	Radius (radius –v on Linux), 3.0.20
	Syslog Server, 3.35.1

	Storage Server Brocade box
	SRC Test OS: Linux distribution conformant to the Brocade company restrictions for external devices. Rocky 9.3

Table 4: Test Setup for independent testing

The overall test result of the independent testing is that no deviations were found between the expected and the actual test results.

7.3. Vulnerability Analysis

Penetration Testing:

The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the ITSEF. Equivalence classes of TOE configurations were identified. At least one TOE configuration of every equivalence class was tested.

SFRs taken from Cryptographic support (FCS), regarding to RNG, SSH and TLS, see [6], chapter 6.1.2. The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment also including an attacker with a *Basic* attack potential.

Attack scenarios having been tested are: Exploiting vulnerabilities in the implementation of TLS, attack scenarios and corresponding results. The test cases cover all attack scenarios for the attack potential *Basic* feasible for the TOE.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential *Basic* was actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

Vulnerability Analysis:

The vulnerability analysis was performed via a CVE analysis of the TOE and its third-party components and penetration testing using the ITSEF's TLS test suite. For the CVE analysis the following publicly available vulnerability databases were used: https://cve-details.com, https://cve.mitre.org, https://nist.gov and https://exploit-db.com. Having performed the vulnerability analysis, the evaluator determined that the TOE is free of exploitable vulnerabilities for the attack potential Basic in the operational environment.

8. Evaluated Configuration

The evaluated configuration is the Brocade Fabric OS, Version 9.1.1b8 software configured as instructed by the preparatory documentation called "BSI Common Criteria Configuration Guide", [9] and pre-installed on Brocade Directors and Switches hardware appliances. By using the preparatory documentation all models run the same configuration of the Fabric OS, Version 9.1.1b8 software.

The Brocade Directors and Switches hardware appliances are available in two form factors:

- a rack-mount Director chassis with a variable number of blades, or
- a self-contained switch appliance device.

The following table summarizes the hardware equivalence classes and the relevant characteristics that distinguish each class:

	EQ I	EQ II	EQ III	EQ IV	EQ V	EQ VI
	Gen 6 Switch Applicance	Gen 6 Director w/ CP blades	Gen 7 Director w/ CP blades	Gen 7 Switch Applicance	Gen 6 Switch Appliance	Gen 7 Switch Applicance
Platforms	G620, 7810	X6-4, X6-8	X7-4, X7-8	G730	G630	G720
Core	e5500	e500mc	e500c	atom	e5500	e5500
Number of cores	2	8	8	2	4	2
Architecture	Power PC	Power PC	Power PC	Intel	Power PC	Power PC
Linux kernel	4.1.35	4.1.35	4.1.35	5.4.66	4.1.35	4.1.35

Table 5: Hardware Equivalence Classes

Note: Downloading and installing Brocade Fabric OS, Version 9.1.1b8 in the field will not lead to an evaluated configuration.

The evaluated configuration does not apply to all the features of the software. Applicable commands to configure or disable excluded features are detailed in the prerequisites and configuration chapters of the guidance documentation [9].

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 31 was used (see [4]).

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The component ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by ALC_FLR.2

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 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only. Note that the column “Security Level” given in table 6 refers to the pure cryptographic (mathematical) strength only, and does not take into account whatever exploitable weaknesses induced by side-channel leakage, physical attacks, or implementation flaws of any kind.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Authenticity	RSA signature generation / verification for TLS RSASSA-PKCS1-v1_5 SHA256, SHA384, SHA512	[17], [30] (SHA), [23] (TLSv1.2)	Modulus length = 2048, 4096 bit	yes for mod length 4096 bit, no for mod length 2048 bit (used for legacy reasons)	FCS_COP.1(4).1
2	Authenticity	ECDSA signature generation / verification using curve P-256, P-384, P-521 for TLS SHA256, SHA384, SHA512	[31] (ECDSA), [30] (SHA), [24] (TLSv1.2)	curve length = 256, 384, 521	yes	FCS_COP.1(5).1
3	Authenticity	RSA signature generation / verification for SSH RSASSA-PKCS1-v1_5 (authentication of SSH Host)	[17], [30] (SHA), [19] (SSH-AUTH)	modulus length = 2048 bit	no (used for legacy reasons)	FCS_COP.1(4).1
4	Authenticity	ECDSA signature generation / verification using curve P-521 for SSH	[31] (ECDSA), [30] (SHA) [25] (ECC for SSH)	Curve length = 521	yes	FCS_COP.1(5).1

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
		(authentication of SSH Host)				
5	Authenticity	Authentication based on user name and password for SSH	Ch. 5 of [19] (SSH-AUTH)	Guess success probability $\varepsilon \leq 10^{-8}$	n/a	FCS_COP.1(3).1
6	Key Agreement	Diffie-Hellman key agreement for SSH (Diffie-Hellman-group16-sha512)	DH KEX with Diffie-Hellman-group16-sha512 MODP from [29], SSH v2.0 KEX from [20]	Plength = 4096	yes	FCS_CKM.2.1, FCS_CKM_EXT.5
7	Key Agreement	ECDH key agreement for SSH (ecdh-sha2-nistp256, ecdhsha2-nistp384, ecdh-sha2-nistp521)	ECDH ([25])	curve length = 256, 384,521	yes	FCS_CKM.2.1, FCS_CKM_EXT.5
8	Key Agreement	Exchange of DH parameters for TLS TLS_ECDHE	ECDHE (TLS_ECDHE) from [24] (TLSv1.2)	curve length = 256, 384,521	yes	FCS_CKM.2.1, FCS_CKM_EXT.5
9	Key Agreement	HMAC value generation for TLS (PRF) HMAC with SHA-256, SHA-384	[30] (SHA), [14] (HMAC), [23] (TLS v1.2)	256 bit and 384 bit	yes	FCS_CKM_EXT.5 Pseudo-Random-Function (PRF) for key derivation tls_prf_sha256 tls_prf_sha384
10	Integrity	HMAC value generation and verification for SSH HMAC with SHA-256, SHA-512	[30] (SHA), [14] (HMAC), [20] (SSH v2.0), [26] (SHA-2 for SSH)	256 bit and 512 bit	yes	FCS_COP.1(2).1 SHA-256, SHA-384, SHA-512 FCS_COP.1(3).1 hmac-sha2-256 hmac-sha2-512
11	Integrity	HMAC value generation and verification for TLS HMAC with SHA-256, SHA-512	[30] (SHA), [14] (HMAC), [23] (TLSv1.2)	256 bit and 512 bit	yes	FCS_COP.1(2).1 FCS_COP.1(3).1
12	Confidentiality	Symmetric encryption and decryption for SSH	[32] (AES), [33] (CBC), [33] (CTR), [34] (GCM), [20]	128 bit, and 256 bit	yes	FCS_COP.1(1).1 aes128-cbc

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
		AES in CBC mode AES in CTR mode AES in GCM mode	(SSH v2.0)			aes256-cbc aes128-ctr aes256-ctr aes128-gcm aes256-gcm
13	Confidentiality	Symmetric encryption and decryption for TLS AES in CBC mode AES in GCM mode	[32] (AES), [33] (CBC), [34] (GCM), [23] (TLS v1.2)	128 bit, and 256 bit	yes	FCS_COP.1(1).1
14	Trusted Channel	SSHv2	[20]	-	yes	FTP_ITC.1, FCS_COP.1(1).1 using the cipher suites aes128-cbc aes256-cbc aes128-ctr aes256-ctr aes128-gcm aes256-gcm
15	Trusted Channel	TLS v1.2[9]	[23]	-	yes	FTP_ITC.1, FCS_COP.1(*) using the cipher suites TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (number C023) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (number C024) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (number C02B)

[9]TLS v1.2 is using STARTTLS

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
						TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (number C02C) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (number C02F) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (number C030) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (number C027) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (number C028)
16	Cryptographic Primitive	CTR_DRBG using AES-256	[39]	-	n/a	FCS_RNG_EXT.1, compliant with functionality class DRG.2 of AIS 20/31 [4]

Table 6: TOE cryptographic functionality

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

AAA Authentication, Authorization and Accounting

AIS Application Notes and Interpretations of the Scheme

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

CA Certificate Authority

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

cPP Collaborative Protection Profile

DMZ Demilitarized Zone

EAL Evaluation Assurance Level

ELP Exchange Link Parameters

ELS Extended Link Service

ETR Evaluation Technical Report

FAN Fabric Address Notification

FC Fibre Channel

FCOE Fibre Channel over Ethernet

FOIP Fibre Channel over IP

FOS Fabric Operating System, Fabric OS

HBA Host Bus Adapter

HTTP Hypertext Transfer Protocol

IP Internet Protocol

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LDAP Lightweight Directory Access Protocol

MUA Multiple User Account

NIC	Network Inferface Card
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-Based Access Control
RFC	Request for Comments
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

Authorized Administrator - A human user who may, in accordance with the TSP, perform an operation after being identified and authenticated.

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[10] 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-1223-2025, Version 1.7, 31 August 2025, Brocade Communications Systems LLC Fabric OS Version 9.1.1b8 Running on Brocade Directors and Switches Security Target, Brocade Communications Systems LLC

[7] Evaluation Technical Report, Version 1.1, 10 September 2025, Evaluation Technical Report (ETR) Summary, SRC Security Research & Consulting (confidential document)

[8] Configuration list for the TOE, Version 5.8, 31 August 2025, Brocade Directors and Switches Configuration Management Plan (confidential document)

[9] Guidance documentation for the TOE, 31 August 2025, Brocade Fabric OS Common Criteria EAL2 User Guide, 9.1.1b8, Publication FOS-91x-CCEAL2-UG100

[10] Brocade Fabric OS - Administration Guide, 9.1.x – Publication FOS-91x-Admin-AG104, January 11, 2024

[11] Brocade Fabric OS Command Reference Manual, 9.1.x, FOS-91x-Command-RM103, January 11, 2024

[12] Brocade Fabric OS Message Reference Manual, 9.1.x, FOS-91x-Message-RM102, January 11, 2024

[10] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren

[13] A proposal for: Functionality classes for random number generators, W. Killmann, W.Schindler, Version 2.0, 01.09.2011

[14] RFC 2104, HMAC: Keyed-Hashing for Message Authentication, Hugo Krawczyk and Mihir Bellare and Ran Canetti, February 1997

[15] RFC 2409, The Internet Key Exchange (IKE), Network Working Group, November 1998

[16] RFC 2865, Remote Authentication Dial In User Service (RADIUS), Network Working Group, June 2000

[17] RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Jakob Jonsson and Burt Kaliski, February 2003

[18] RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), Network Working Group, May 2003

[19] RFC 4252, The Secure Shell (SSH) Authentication Protocol, Chris M. Lonvick and Tatu Ylonen, January 2006

[20] RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, Network Working Group, January 2006

[21] RFC 4511, Lightweight Directory Access Protocol (LDAP): The Protocol, Network Working Group, June 2006

[22] RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, Network Working Group, January 2008

[23] RFC 5246, The Transport Layer Security (TLS) Protocol, Version 1.2, Network Working Group, August 2008

[24] RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), Eric Rescorla, August 2006

[25] RFC 5656, Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer, Douglas Stebila and Jonathan Green, December 2009

[26] RFC 6668, SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol, Mark D. Baushke and Denis Bider, July 2012

[27] RFC 7027, Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), Internet Engineering Task Force, October 2013

[28] RFC 7919, Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS), Network Working Group, August 2016

[29] RFC 8268, More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH), October 2017

[30] FIPS PUB 180-4, Secure Hash Standard (SHS), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, August 2015

[31] FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology, July 2013, Mark D. Baushke, December 2017

[32] FIPS PUB 197, Advanced Encryption Standard, U.S. Department of Commerce / National Institute of Standards and Technology, February 2001

[33] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Morris J. Dworkin, National Institute of Standards & Technology, December 2001

[34] NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Morris J. Dworkin, National Institute of Standards & Technology, November 2007

[35] Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, and S. Vanstone. CRC Press, 2001

[36] https://github.com/RUB-NDS/TLS-Attacker, Version 2.6

[37] Lucky Thirteen: Breaking the TLS and DTLS Record Protocols, Nadhem J. AlFardan and Kenneth G. Paterson, February 2013

[38] Certification Path Validation Test Tool—Test Specification, BSI, February 2018

[39] NIST SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Elaine Barker and John Kelsey, National Institute of Standards & Technology, June 2015

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.

Note: End of report