Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0969-2015

for

Brocade Communications Systems, Inc. FabricOS Version: 7.3.0a3

from

Brocade Communications Systems, Inc.

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-0969-2015 (*)

Network and Network related Devices and Systems

Brocade Communications Systems, Inc. FabricOS
Version: 7.3.0a3

from	Brocade Communications Systems, Inc.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 extended EAL 2 augmented by ALC_FLR.2

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 4

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, 8 December 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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.

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

Contents

A. Certification

1. 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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [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]

2. 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.

2.1. European Recognition of ITSEC/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.

---

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

3 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

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). 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 new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

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

2.2. 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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://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 nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

3. 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 Brocade Communications Systems, Inc. FabricOS, Version: 7.3.0a3 has undergone the certification procedure at BSI.

The evaluation of the product Brocade Communications Systems, Inc. FabricOS, Version: 7.3.0a3 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 19 November 2015. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: Brocade Communications Systems, Inc..

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

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 December 2015 is valid until 7 December 2020. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,

[6] Information Technology Security Evaluation Facility

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.

5. Publication

The product Brocade Communications Systems, Inc. FabricOS, Version: 7.3.0a3 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
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 product Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3 running on Brocade Directors and Switches family of products. They are configured as instructed by the preparatory documentation described in [9], [10], [11], [12] and [13] which are provided by Brocade Communications Systems, Inc.. Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3 running on Brocade Directors and Switches 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 and 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 (HBA). 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 [14] or LDAP [15] server. Passwords are chosen by a defined policy.
Security Management	The TOE provides both serial terminal- and Ethernet network-based

TOE Security Functionality	Addressed issue
	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. Based on these assets the TOE Security Problem is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapters 3.1 and 3.2.

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

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Brocade Communications Systems, Inc. FabricOS, Version: 7.3.0a3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3	7.3.0a3	Pre-installed on Brocade Director Blade Models, Director Models and Switch Appliance Models (see list below)
2	DOC	Brocade FabricOS v7.3.0a3 BSI Common Criteria Configuration Guide [9] SHA512 checksum: 155E7DB166A31DC8A8BA632DF174AC6CA39EC97DA31215317ACACD414EC3AA70804FDCB5BA15A0BB7474D3D9E5288AC31A66AF140C98C6C695672479C32E9108	#53-1003807-02, 21 October 2015	Password-protected user-id for registered users (customers), web download secured with https

No	Type	Identifier	Release	Form of Delivery
3	DOC	Brocade - FabricOS Administrator's Guide [10] SHA512 checksum: 4DAF5FBFF885E23B50B26F1D72E21449A6B4D8A67CDB8EE225DC18BBE2E617D04CFFC88EF6781ADB65D957049FFF4FEA6ED6B087D7A60674C925F977779EB798	#53-1003130-01, 27 June 2014	Password-protected user-id for registered users (customers), web download secured with https
4	DOC	Brocade – FabricOS Command Reference [11] SHA512 checksum: C0D3ED09340AEFEB6DD2B8BA6F595D7CBAE924D3A462DE6C4468CCB72AC099ED276BE468E415C9112C00F371A2269CA1B75B87EDB62DE548E433150CC6FB24FE	#53-103131-01, 27 June 2014	Password-protected user-id for registered users (customers), web download secured with https
5	DOC	Brocade – FabricOS Message Reference [12] SHA512 checksum: A5281B722D4C2858178B2D62CBB8AEB3519876952825A8343FCACFD7897020F306E7BF6F2D546008B75228F36ED118E532AE9B9B4BBDF98B48D4A03236D4C589	#53-1003140-01, 27 June 2014	Password-protected user-id for registered users (customers), web download secured with https
6	DOC	Brocade – FabricOS Troubleshooting and Diagnostics Guide, Supporting FabricOS v7.3.0 [13] SHA512 checksum: DCA5B42E5EFD994B7F913AE0DAB0814EF0D50FF515655B4B34BA8B8A6219B73DEBF8EE37A17C1C193A8E4D554C99CAB94A66103860A027ECCC738A15D2BF765F	#53-1003141-02, 15 August 2014	Password-protected user-id for registered users (customers), web download secured with https

Table 2: Deliverables of the TOE

The certified software, Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3, is certified for the following series and models of Brocade Director and switch products:

- Director Blade Models: FC16-32, FC16-48, FC16-64, CP8,CR16-4, CR16-8, FX8-24
- Director Models: DCX 8510-4, DCX 8510-8
- Switch Appliance Models: 6505, 6510, 6520, 7800, 7840

The software loading process is automated and solely controlled by Brocade's engineers. Brocade FabricOS images are retrieved by authorized Brocade personnel and are transferred securely to factory sites across private networks. After the hardware is loaded with FabricOS at the manufacturer´s site, the hardware is packaged with tamper-proof security tape 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.

This shrink-wrapped crate is shipped to Brocade's OEM/channel partners and 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.

In the case that Brocade performs the delivery to end customers directly, transport is per-formed by trusted C-TPAT certified carriers. 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 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.

For documentation 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 with user-ID and password which are provided only to these registered users. This documentation is authored by Brocade and transferred to the Brocade web site (http://www.brocade.com) through a VPN that provides authentication of Brocade as the document's source. The web download of the documentation files is secured with Hypertext Transfer Protocol Secure (HTTPS).

Note 1: It is unequivocally stated in the BSI Common Criteria Configuration Guide [9] that the download delivery which is also offered by the developer does not lead to a certified version of the TOE.

Note 2: Using the BSI Common Criteria Configuration Guide [9] with a downloaded version of FabricOS will not lead to a certified version.

2.1. Identification of the TOE by the User

On boot up, the user has to verify and confirm that the approved Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3 is pre-installed using the 'firmwareshow' command.

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

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:

- 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 [6].
- 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 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 1.2, [6]. In particular it is assumed that the following functionality is available to the TOE:

  a) Hardware real time clock

  b) A trustworthy bootloader

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

5. Architectural Information

The Target of Evaluation (TOE) is Fabric Operating System (FabricOS) version 7.3.0a3 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 the evaluation.

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

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

Operating system capabilities of the FabricOS are executed by the Runtime Subsystem. The Runtime Subsystem provides an execution environment for the FabricOS 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 and
- an IP filtering capability.

The FabricOS subsystem provides the following major capabilities:

- logging functionality,
- crypto support functionality,
- admin functionality,
- AAA functionality,
- remote access functionality and
- 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 cyrptographic operations associated with various network protocols (e.g., SSHv2, TLSv1.2). The crypto support functionality also generates SSH & TLS keys.

The admin functionality provides a Command Line Interface (CLI) for the configuration and management of the FabricOS subsystem over an SSH connection and ensures that all users are identified and authenticated before being allowed to perform operations using the 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.

The AAA functionality provides network protocol support for the RADIUS and LDAP protocols. These protocols connect the FabricOS subsystem with an external authentication server. The Runtime Environment provides a local repository for user identification and authentication material. Together, the FabricOS subsystem can utilize either locally defined accounts or accounts defined via LDAP and RADIUS for the identification and authentication of administrators.

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 FabricOS subsystem.

All networking performed by the FabricOS 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 FabricOS Subsystem with HBAs and storage devices.

The SAN functionality implements the FabricOS 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 FabricOS 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 FabricOS subsystem, and to support communication with external syslog, RADIUS and LDAP servers.

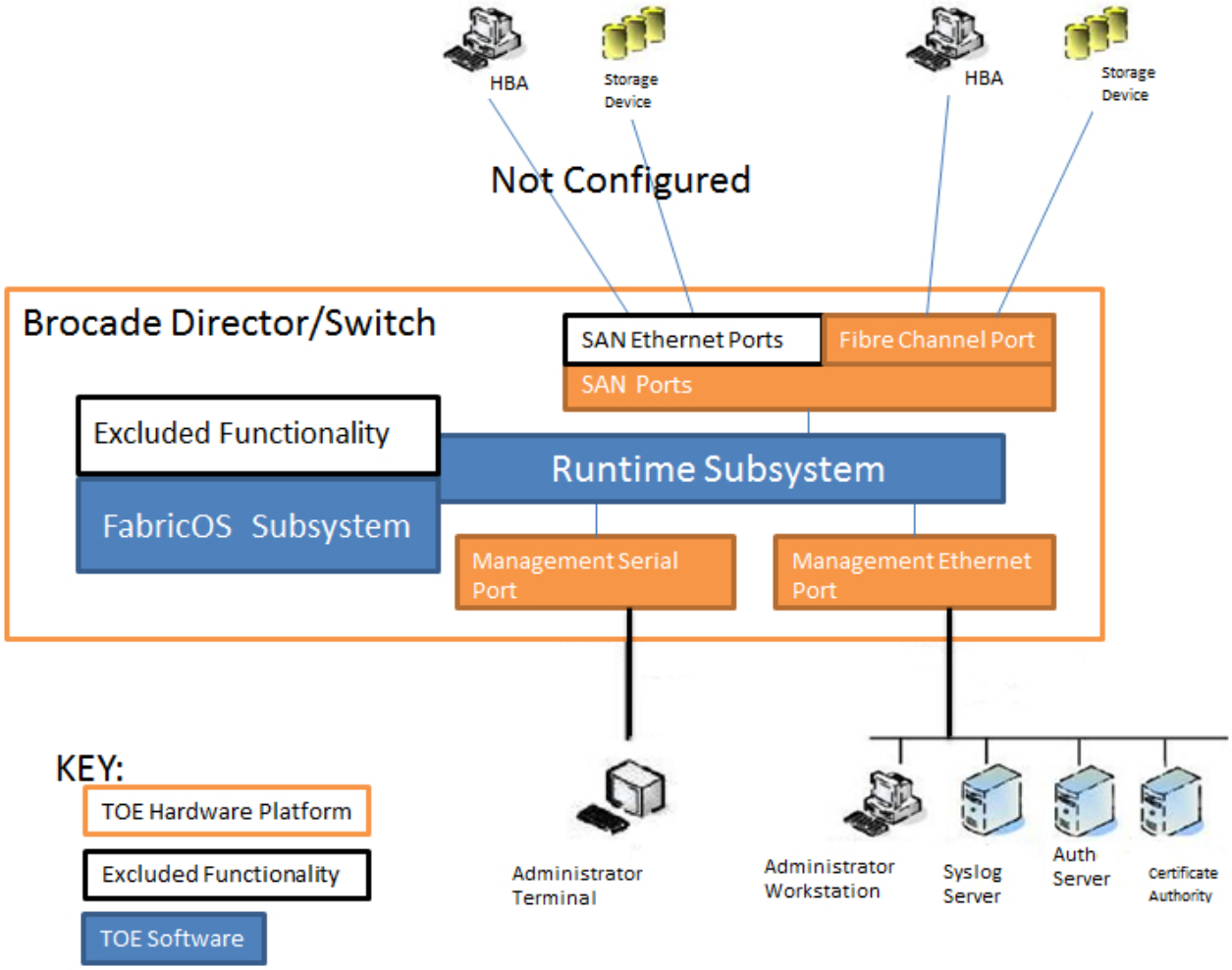

Figure 1: TOE Architecture

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 Tests

Test Configuration and Test Approach

Brocade FabricOS 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, 7840 equivalence class or Director equivalence class. Tests are executed on every equivalence class (later also referred to as “Eq Cl”). See Table 4 in Chapter 8 for details.

For testing purpose the TOE is configured following strictly the referenced BSI Common Criteria Configuration Guide [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 in the Security Target claimed security features.

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.

Test Cases and Results

- Enable security auditing (FAU_GEN.1): This test enables security auditing and verifies that set security alerts are triggered and reported correctly to the syslog server.
- Account lockout for non admin accounts and 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 those of user role.
- Authenticate incoming and outgoing SSH user with RSA keys (FCS_CKM.1(2).1, FCS_COP.1(2), FCS_CKM.1(1).1): Validation of RSA key authentication to and from the FOS switch without a password.
- Key and secret creation and deletion (FCS_CKM.4): This test verifies that certificates can be deleted successfully.
- Basic zoning on different hardware (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): Validation of the correct cipher suites in SSH and all TLS sessions.
- Maximum number of sessions for each role and closing of active sessions (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.
- Verify import utility for validity of a certificate (FIA_ATD.1(1)): This test verifies that invalid certificates cannot be imported into FOS for use with LDAP or the syslog server.

7.2. Independent Evaluator Tests

Overview

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

TOE Test Configuration

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 [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 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 1.4.2 [6] (OE.CONFIG). Tests are executed only with Brocade Directors and Switches that are listed in section 1.2 [6] (OE.HARDWARE).

These above described components match the needed components described in the BSI Common Criteria Configuration Guide [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 three appliances, one of each equivalence class with an redundant appliance. The four

workstations represent the two authentication servers, syslog server and a testing work-station. The entire developer test configuration and the test protocols were made avail-able to the evaluator.

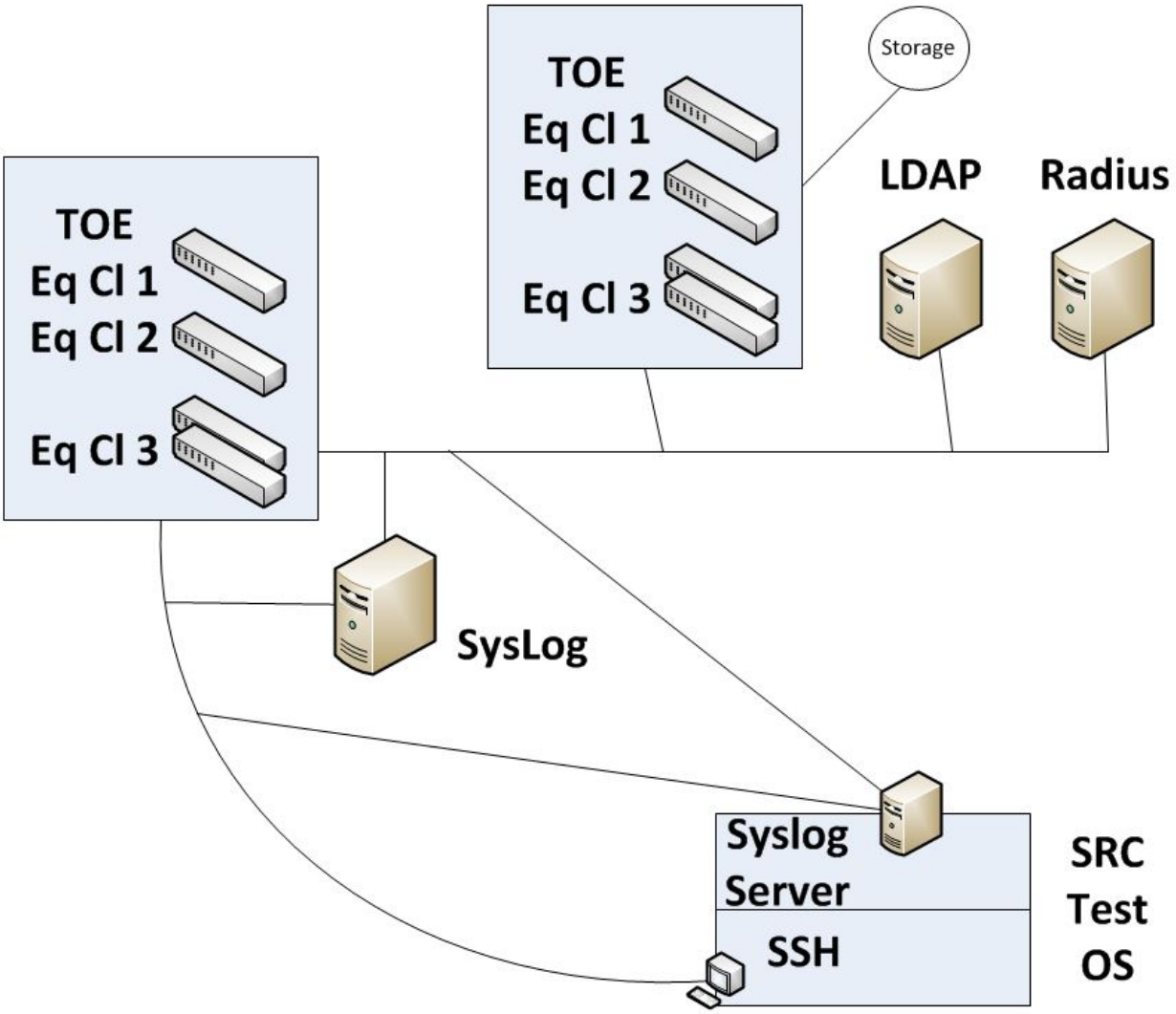

Figure 2: Test Environment

For testing the TOE the evaluators used the same configuration as used in the developer tests. The machines and the developer test cases were analysed during a visit of SRC in the test lab of Brocade in Denver (CO) USA. After that a remote connection to a test DMZ was installed on a separated network segment at Brocade. The network configuration was not changed by the evaluators. The description of the required non-TOE hardware, software and firmware is described in section 1.4.2 of [6]. During the visit the evaluators used the following test configuration:

Hardware	7800 (Eq Cl1) 7840 (Eq Cl2) DCX CP0 / CP1 (Eq Cl3) 8510-4
Software	Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3
	LDAP Linux: OpenLDAP: slapd 2.4.23 Windows Server 2012 R2 Datacenter: AD DS (Active Directory Domain Services)

Hardware	7800 (Eq Cl1) 7840 (Eq Cl2) DCX CP0 / CP1 (Eq Cl3) 8510-4
	RADIUS Linux: FreeRadius Version 2.1.5 Windows Server 2012 R2 Datacenter: RADIUS Client in Network Access Policy
	SYSLOG Server syslog-ng 3.5.6 on Debian 3.7.2-0 Linux and on kali8 x86_64 Linux
	Storage Server SANBlaze V7.2-64-3.5.0
	SRC Test OS Kali Linux Version 3.14-kali-amd64

Table 3: Test Configuration

This hardware and software configuration has been used to establish a complete testing network including the TOE in every equivalence class.

During the tests the TOE runs on three different hardware appliances according to each equivalence class. In most of the test cases the TOE communicates with a server (LDAP, RADIUS or syslog). Additionally, the TOE has been set up between the systems and SRC to conduct the evaluator tests. The systems are connected using Ethernet connection.

Test Cases and Results

All developer tests were redone during the visit of the test lab in Denver (CO) USA from 8th to 13th of March 2015. The following list shows six of the conducted developer tests as examples:

- Login via SSH as LDAP user and verify that login is successful.
- 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.
- Delete private key and known hosts.
- Create an initial Zone on the switch.
- Expire user password of ‘user’.

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

The following list briefly summarizes the test subset devised by the evaluator:

- Try to connect TOE to server with imported certificate (Positive Test)
- Try to connect TOE to server with imported certificate and wrong cipher (Negative Test)
- Try to connect TOE to server with manipulated certificate on Syslog Server (Negative Test)
- Try to establish SSH connection to TOE (Positive Test)
- Try to establish SSH connection to TOE after deleting known hosts (Positive Test)
- Test of the SSH connection timeout after establishment (Positive Test)

- Test of the dev/random function (Negative Test)

The independent test subset consists of six individual tests. The first and last test case were executed during the AVA penetration tests.

All actual test results were consistent with the expected test results.

7.3. Vulnerability Analysis

Overview

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.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic was actually successful.

The same test configuration as shown in table 3 was used.

Tests and Results

All SFRs taken from Cryptographic Support (FCS) regarding to RNG, SSH and TLS were penetration tested. The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment and assuming an attacker with a Basic attack potential.

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.

Having performed the vulnerability analysis, the evaluator determined that the TOE is free of exploitable vulnerabilities as well as residual vulnerabilities.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The evaluated configuration is the Brocade FabricOS version 7.3.0a3 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.

The various models of the hardware supporting the TOE are mentioned in Chapter 2. By using the preparatory documentation all models run the same configuration of the FabricOS Version 7.3.0a3 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:

	7840	Switch Appliance	Director w/ CP blades
Platforms	7840	6505, 6510, 6520, 7800	DCX 8510-4, DCX 8510-8
ASIC	Goldeneye2	Goldeneye2 and Condor3	Condor3
Speed	16Gb	4G to 16Gb	4G to 16Gb
Credit Buffers	700	8192	8192
SID CAM Table Size	n/a	n/a	n/a
DID CAM Table Size	n/a	n/a	n/a
Zones	4K	8K	8K
Max Trunk Ports	8	8	8

Table 4: Deliverables of the TOE

The evaluated configuration does not apply to all the features of the software. The following is a list of product features that are excluded from the evaluation and must be disabled or not configured for use in the TOE configuration:

- Redundancy or encryption provided by processing of user data by ASICs is not evaluated.
- Fibre Channel over Ethernet (FCOE) cannot be configured to create SAN Ethernet Ports.
- Fibre Channel over IP (FCIP) cannot be configured for use over SAN Ethernet Ports.
- The TOE is configured to exclude the use of Elliptic-Curve Cryptographic algorithms for use with SSH by the use of certificates and keys defined using Elliptic-Curve Cryptographic algorithms.
- Web-based administrator console interfaces called the “Brocade Advanced Web Tools” cannot be used for administration of the TOE.
- The SNMP administrative interface cannot be used and must be disabled.
- Optional modem hardware for simulating a serial administration interface is not installed.
- The TOE cannot be operated in Access Gateway mode.
- Dynamic RBAC is not configured for use by administrators.
- Insecure protocols such as FTP and Telnet must not be used (or must be disabled) per instructions in the guidance.
- IPsec features have not been evaluated and must be disabled per guidance instructions.
- Additionally, the TOE cannot be configured to prevent the use of Elliptic-Curve Cryptographic algorithms supporting TLS other than by not creating (or deleting any existing) certificates and keys based on Elliptic-Curve Cryptographic algorithms. The Elliptic-Curve Cryptographic algorithms have not been evaluated.
- Note that the Brocade Network Advisor is a management tool which utilizes the SNMP and web interfaces to communicate with the TOE. However, because both of those interfaces are excluded, then the Brocade Network Advisor is also excluded

Applicable commands to configure or disable excluded features are detailed in the pre-requisites and configuration chapters of the BSI Common Criteria Configuration Guide, [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 AIS 31 were 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 components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None [8]
- 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 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).

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).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	SSH: Key Exchange	DH ([HaC]) with Diffie-Hellman-group1 4-sha1	[RFC4253] (SSH v2.0), [RFC3526] (MODP)	2048	yes
2	TLS: encrypted exchange of pre-master secret	RSA-encryption RSAES-PKCS1-v1_5 (TLS_RSA)	[RFC5246] (TLS v1.2), [PKCS#1 v2.1]	2048	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
3	SSH Encryption and decryption	SSH: AES in CBC mode (aes128-cbc, aes256-cbc)	[FIPS-197] (AES), [SP 800-38A] (CBC), [RFC4253] (SSH v2.0)	128, 256	yes
4	SSH Message authentication code generation and verification	SSH: HMAC with SHA-256, SHA-512 (hmac-sha2-256, hmac-sha2-512)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC4253] (SSH v2.0), [RFC6668] (SHA-2 for SSH)	256, 512	yes
5	TLS Encryption and decryption	TLS: AES in CBC mode (AES_128_CBC, AES_256_CBC)	[FIPS-197] (AES), [SP 800-38A] (CBC), [RFC5246] (TLS v1.2)	128, 256	yes
6	TLS Message authentication code generation and verification	TLS: HMAC with SHA-1 or SHA-256 (SHA1, SHA256)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	160, 256	yes
7	SSH Server and client: Authentication of user	generation (“publickey”: RSASSA-PKCS1-v1_5)	PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC4252] (SSH-AUTH)	modulus length ≥ 2048	yes
		Authentication based on user name and password (“password”)	ch. 5 of [RFC4252] (SSH-AUTH)	Guess success probability $\varepsilon \leq 10^{-8}$	no
8	SSH Client: Authentication of host	RSA signature verification (RSASSA-PKCS1-v1_5 using SHA1(rsa2048-sha1))	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC4432] (RSA for SSH)	modulus length = 2048	yes
8	TLS: Asymmetric authentication	Public-key-based authentication of the server using RSA-encryption RSAES-PKCS1-v1_5 using SHA-1	[PKCS#1 v2.1], [FIPS180-4] (SHA), [RFC5246] (TLS v1.2)	Modulus length = 2048	no
9	SSH Key Derivation Function	SSH: PRF based on SHA-1 (diffie-hellman-group14-sha1)	[FIPS180-4] (SHA), [RFC4253] (SSH v2.0)	|K| = variable	yes
10	TLS Key Derivation Function	TLSv1.2: PRF based on HMAC with SHA-256 (tls_prf_sha256)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	|K| = variable	yes
11	TLS Key	TLSv1.2: PRF based	[FIPS180-4] (SHA),	|K| = variable	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	Derivation Function	on HMAC with SHA-384 (tls_prf_sha384)	[RFC2104] (HMAC), [RFC5246] (TLS v1.2)		

Table 5: 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.

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.

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.

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CLI Command Line Interface

cPP Collaborative Protection Profile

DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FC	Fiber Channel
FCOE	Fibre Channel over Ethernet
FCIP	Fibre Channel over IP
HBA	Host Bus Adapter
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-Based Access Control
SAN	Storage Area Network
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.

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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[8] 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-0969-2015, Version 1.0, October 21, 2015, Brocade Communications Systems, Inc. FabricOS Version 7.3.0a3 running on Brocade Directors and Switches Security Target, Brocade Communications Systems, Inc.

[7] Evaluation Technical Report, Version 1.2, November 19, 2015, Evaluation Technical Report (ETR) Summary, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration list for the TOE, 16, October 21, 2015, Brocade Configuration Management Plan (confidential document)

[9] Brocade FabricOS v7.3.0a3 BSI Common Criteria Configuration Guide, Publication 53-1003807-02, October 21, 2015

[10] FabricOS Administrator's Guide, Publication #53-1003130-01, June 27, 2014

[11] FabricOS Command Reference, Publication #53-103131-01, June 27, 2014

[12] FabricOS Message Reference, Publication #53-1003140-01, June 27, 2014

[13] Troubleshooting and Diagnostics guide – Supporting Fabric OS v7.3.0, Publication #53-1003141-02, August 15, 2014

[14] RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.

[15] RFC 4511, Lightweight Directory Access Protocol (LDAP): The Protocol, June 2006.

[8] 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

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.