Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0999-2016

for

Red Hat Enterprise Linux Version 7.1

from

Red Hat

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-0999-2016 (*)

Operating System

Red Hat Enterprise Linux
Version 7.1

from	Red Hat
PP Conformance:	Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010, OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

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, 26 September 2016

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 this certificate is a re-certification of a certificate issued according to CCRA-2000 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 Red Hat Enterprise Linux, Version 7.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0754-2012. Specific results from the evaluation process BSI-DSZ-CC-0754-2012 were re-used.

The evaluation of the product Red Hat Enterprise Linux, Version 7.1 was conducted by atsec information security GmbH. The evaluation was completed on 30 June 2016. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Red Hat.

The product was developed by: Red Hat.

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 26 September 2016 is valid until 25 September 2021. 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

---

6 Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

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

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

5. Publication

The product Red Hat Enterprise Linux, Version 7.1 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 Red Hat
100 East Davie Street
Raleigh, NC 27601
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 Red Hat Enterprise Linux, Version 7.1.

Red Hat Enterprise Linux is a highly-configurable Linux-based operating system which has been developed to provide a good level of security as required in commercial environments. It also meets all requirements of the Operating System protection profile [OSPP]. Additional functionality to the OSPP base is claimed:

- Advanced Management (MLS mode only)
- Labeled Security (MLS mode only)
- Runtime protection against programming errors
- Packet Filter
- Linux Container Framework Support (not on POWER architecture)

The TOE can operate in two different modes of operation called “Base mode” and “MLS mode”. In Base mode, the SELinux security module does not enforce a mandatory access control policy for the general computing environment and does not recognize sensitivity labels of subjects and objects. SELinux can either be disabled completely, or enabled with a non-MLS policy which only add additional restrictions to the base access control functions without interfering with the “root” administrator role. In this mode the TOE enforces all security requirements of the OSPP [8].

SELinux must be enabled if the administrator wants to provide virtual machines. In MLS mode, the SELinux security module is configured to enforce the mandatory access control policy based on the labels of subjects and objects as required by the extended OSPP packages for labeled security [8] as well as advanced management [8].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile and Extended Packages

Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010, OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010 [8].

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 4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.3. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
Auditing	The Lightweight Audit Framework (LAF) is designed to be an audit system making Linux compliant with the requirements from Common Criteria. LAF is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem

TOE Security Functionality	Addressed issue
	allows configuring the events to be actually audited from the set of all events that are possible to be audited.
Cryptographic support	The TOE provides cryptographically secured communication channels as well as cryptographic primitives that unprivileged users can utilize for unspecified purposes. The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. For interactive usage, the SSHv2 protocol is provided. Using OpenSSH, password-based and public-key-based authentication are allowed.
Packet filter	The TOE provides a stateless and stateful packet filter for regular IP-based communication. OSI Layer 3 (IP) and OSI layer 4 (TCP, UDP, ICMP) network protocols can be controlled using this packet filter. To allow virtual machines to communicate with the environment, the TOE provides a bridging functionality. Ethernet frames routed through bridges are controlled by a separate packet filter which implements a stateless packet filter for the TCP/IP protocol family.
Identification and Authentication	User identification and authentication in the TOE includes all forms of interactive login (e.g. using the SSH protocol or log in at the local console) as well as identity changes through the su or sudo command. These all rely on explicit authentication information provided interactively by a user.
Discretionary Access Control (DAC)	DAC allows owners of named objects to control the access permissions to these objects. These owners can permit or deny access for other users based on the configured permission settings. The DAC mechanism is also used to ensure that untrusted users cannot tamper with the TOE mechanisms.
Mandatory Access Control (MAC)	The TOE supports mandatory access control.
Security Management	The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of TSF.
Runtime Protection Mechanisms	The TOE provides mechanisms to prevent or significantly increase the complexity of an exploitation of common buffer overflow and similar attacks. These mechanisms are used for the TSF and are available to untrusted code.
Linux Container Framework Support (not on POWER architecture)	Linux Containers provide execution environments for processes. These Linux Containers isolate the processes, ensure resource accounting and limitation as well as Linux kernel service limitation.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.3.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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:

Red Hat Enterprise Linux, Version 7.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Red Hat Enterprise Linux 7.1 Server, x86_64 Architecture rhel-server-7.1-x86_64-dvd.iso SHA-256 Checksum: 3685468ec6cdcb70dfc85ebbc164da427dc2d762644c3c2ee1520f4f661c15ce	7.1	Download
2	SW	Red Hat Enterprise Linux 7.1 Server, ppc64 Architecture rhel-server-7.1-ppc64-dvd.iso SHA-256 Checksum: 021d7db257ba9242e6408fbd308daacf58302d6bc32158e6bef50b13d7ed3f79	7.1	Download
3	SW	Red Hat Enterprise Linux 7.1 Server, ppc64le Architecture rhel-server-7.1-ppc64le-dvd.iso SHA-256 Checksum: 357e4df56b71356c5c9e2c916cf412a048350b386926840365b0769894460fa1	7.1	Download
4	SW	Red Hat Enterprise Linux 7.1 Server, s390x Architecture rhel-server-7.1-s390x-dvd.iso SHA-256 Checksum: 2334c1aa0bdc1be41b1c53b6a823bd98ea78b1bfd030c5587764e9caa7fedfe9	7.1	Download
5	SW / DOC	Evaluation package RPM EAL4_RHEL7.1, including the "Evaluated Configuration Guide" ([10]) cc-config-rhel71-*.rpm	7.1	Download

No	Type	Identifier	Release	Form of Delivery
6	SW (x86_64)	**Additional RPMs for x86_64** bind-libs-9.9.4-18.el7_1.2.x86_64.rpm, bind-libs-lite-9.9.4-18.el7_1.2.x86_64.rpm, bind-license-9.9.4-18.el7_1.2.noarch.rpm, bind-utils-9.9.4-18.el7_1.2.x86_64.rpm, binutils-2.23.52.0.1-30.el7_1.2.x86_64.rpm, ca-certificates-2015.2.4-70.0.el7_1.noarch.rpm, cups-1.6.3-17.el7_1.1.x86_64.rpm, cups-client-1.6.3-17.el7_1.1.x86_64.rpm, cups-filesystem-1.6.3-17.el7_1.1.noarch.rpm, cups-libs-1.6.3-17.el7_1.1.x86_64.rpm, device-mapper-1.02.93-3.el7_1.1.x86_64.rpm, device-mapper-event-1.02.93-3.el7_1.1.x86_64.rpm, device-mapper-event-libs-1.02.93-3.el7_1.1.x86_64.rpm, device-mapper-libs-1.02.93-3.el7_1.1.x86_64.rpm, lvm2-2.02.115-3.el7_1.1.x86_64.rpm, lvm2-libs-2.02.115-3.el7_1.1.x86_64.rpm, dnsmasq-2.66-13.el7_1.x86_64.rpm, dracut-033-241.el7_1.5.x86_64.rpm, dracut-config-rescue-033-241.el7_1.5.x86_64.rpm, dracut-network-033-241.el7_1.5.x86_64.rpm, freetype-2.4.11-10.el7_1.1.x86_64.rpm, glibc-2.17-79.el7_1.4.x86_64.rpm, glibc-common-2.17-79.el7_1.4.x86_64.rpm, gnutls-3.3.8-12.el7_1.1.x86_64.rpm, hwdata-0.252-7.8.el7_1.x86_64.rpm, iputils-20121221-6.el7_1.1.x86_64.rpm, kernel-3.10.0-229.26.2.el7.x86_64.rpm, kernel-headers-3.10.0-229.26.2.el7.x86_64.rpm, kernel-tools-3.10.0-229.26.2.el7.x86_64.rpm, kernel-tools-libs-3.10.0-229.26.2.el7.x86_64.rpm, kexec-tools-2.0.7-19.el7_1.2.x86_64.rpm, libgcrypt-1.5.3-12.el7_1.1.x86_64.rpm, libpcap-1.5.3-4.el7_1.2.x86_64.rpm, libreswan-3.12-10.1.el7_1.x86_64.rpm, libuser-0.60-7.el7_1.x86_64.rpm, libxml2-2.9.1-5.el7_1.2.x86_64.rpm, libxml2-python-2.9.1-5.el7_1.2.x86_64.rpm, nspr-4.10.8-2.el7_1.x86_64.rpm, nss-3.19.1-5.el7_1.x86_64.rpm, nss-sysinit-3.19.1-5.el7_1.x86_64.rpm, nss-tools-3.19.1-5.el7_1.x86_64.rpm, nss-util-3.19.1-5.el7_1.x86_64.rpm, nss-softokn-3.16.2.3-13.el7_1.x86_64.rpm, nss-softokn-freebl-3.16.2.3-13.el7_1.x86_64.rpm, openssh-6.6.1p1-12.el7_1.x86_64.rpm, openssh-clients-6.6.1p1-12.el7_1.x86_64.rpm, openssh-keycat-6.6.1p1-12.el7_1.x86_64.rpm, openssh-server-6.6.1p1-12.el7_1.x86_64.rpm, openssl-1.0.1e-42.el7_1.9.x86_64.rpm, openssl-libs-1.0.1e-42.el7_1.9.x86_64.rpm, python-2.7.5-18.el7_1.1.x86_64.rpm, python-libs-2.7.5-18.el7_1.1.x86_64.rpm, samba-libs-4.1.12-23.el7_1.x86_64.rpm, libwbclient-4.1.12-23.el7_1.x86_64.rpm, selinux-policy-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-devel-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-mls-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-targeted-3.13.1-23.el7_1.8.noarch.rpm, libipa_hbac-1.12.2-58.el7_1.14.x86_64.rpm, libsss_idmap-1.12.2-58.el7_1.14.x86_64.rpm, libsss_nss_idmap-1.12.2-58.el7_1.14.x86_64.rpm, sssd-client-1.12.2-58.el7_1.14.x86_64.rpm, sssd-common-1.12.2-58.el7_1.14.x86_64.rpm, sssd-common-pac-1.12.2-58.el7_1.14.x86_64.rpm, sssd-ipa-1.12.2-58.el7_1.14.x86_64.rpm, sssd-krb5-common-1.12.2-58.el7_1.14.x86_64.rpm, systemd-208-20.el7_1.5.x86_64.rpm, systemd-libs-208-20.el7_1.5.x86_64.rpm, systemd-sysv-208-20.el7_1.5.x86_64.rpm, libgudev1-208-20.el7_1.5.x86_64.rpm, trousers-0.3.11.2-4.el7_1.x86_64.rpm, tzdata-2015e-1.el7.noarch.rpm, util-linux-2.23.2-22.el7_1.x86_64.rpm, libblkid-2.23.2-22.el7_1.x86_64.rpm, libmount-2.23.2-22.el7_1.x86_64.rpm, libuuid-2.23.2-22.el7_1.x86_64.rpm, wpa_supplicant-2.0-17.el7_1.x86_64.rpm, dracut-fips-033-241.el7_1.3.x86_64.rpm, dracut-fips-aesni-033-241.el7_1.3.x86_64.rpm	see package names	Download

No	Type	Identifier	Release	Form of Delivery
7	SW (s390x)	**Additional RPMs for s390x** bind-libs-9.9.4-18.el7_1.2.s390x.rpm, bind-libs-lite-9.9.4-18.el7_1.2.s390x.rpm, bind-license-9.9.4-18.el7_1.2.noarch.rpm, bind-utils-9.9.4-18.el7_1.2.s390x.rpm, binutils-2.23.52.0.1-30.el7_1.2.s390x.rpm, ca-certificates-2015.2.4-70.0.el7_1.noarch.rpm, cups-1.6.3-17.el7_1.1.s390x.rpm, cups-client-1.6.3-17.el7_1.1.s390x.rpm, cups-filesystem-1.6.3-17.el7_1.1.noarch.rpm, cups-libs-1.6.3-17.el7_1.1.s390x.rpm, device-mapper-1.02.93-3.el7_1.1.s390x.rpm, device-mapper-event-1.02.93-3.el7_1.1.s390x.rpm, device-mapper-event-libs-1.02.93-3.el7_1.1.s390x.rpm, device-mapper-libs-1.02.93-3.el7_1.1.s390x.rpm, lvm2-2.02.115-3.el7_1.1.s390x.rpm, lvm2-libs-2.02.115-3.el7_1.1.s390x.rpm, dnsmasq-2.66-13.el7_1.s390x.rpm, dracut-033-241.el7_1.5.s390x.rpm, dracut-config-rescue-033-241.el7_1.5.s390x.rpm, dracut-network-033-241.el7_1.5.s390x.rpm, freetype-2.4.11-10.el7_1.1.s390x.rpm, glibc-2.17-79.el7_1.4.s390x.rpm, glibc-common-2.17-79.el7_1.4.s390x.rpm, gnutls-3.3.8-12.el7_1.1.s390x.rpm, hwdata-0.252-7.8.el7_1.s390x.rpm, iputils-20121221-6.el7_1.1.s390x.rpm, kernel-3.10.0-229.26.2.el7.s390x.rpm, kernel-headers-3.10.0-229.26.2.el7.s390x.rpm, kexec-tools-2.0.7-19.el7_1.2.s390x.rpm, libgcrypt-1.5.3-12.el7_1.1.s390x.rpm, libpcap-1.5.3-4.el7_1.2.s390x.rpm, libreswan-3.12-10.1.el7_1.s390x.rpm, libuser-0.60-7.el7_1.s390x.rpm, libxml2-2.9.1-5.el7_1.2.s390x.rpm, libxml2-python-2.9.1-5.el7_1.2.s390x.rpm, nspr-4.10.8-2.el7_1.s390x.rpm, nss-3.19.1-5.el7_1.s390x.rpm, nss-sysinit-3.19.1-5.el7_1.s390x.rpm, nss-tools-3.19.1-5.el7_1.s390x.rpm, nss-util-3.19.1-5.el7_1.s390x.rpm, nss-softokn-3.16.2.3-13.el7_1.s390x.rpm, nss-softokn-freebl-3.16.2.3-13.el7_1.s390x.rpm, openssh-6.6.1p1-12.el7_1.s390x.rpm, openssh-clients-6.6.1p1-12.el7_1.s390x.rpm, openssh-keycat-6.6.1p1-12.el7_1.s390x.rpm, openssh-server-6.6.1p1-12.el7_1.s390x.rpm, openssl-1.0.1e-42.el7_1.9.s390x.rpm, openssl-libs-1.0.1e-42.el7_1.9.s390x.rpm, python-2.7.5-18.el7_1.1.s390x.rpm, python-libs-2.7.5-18.el7_1.1.s390x.rpm, samba-libs-4.1.12-23.el7_1.s390x.rpm, libwbclient-4.1.12-23.el7_1.s390x.rpm, selinux-policy-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-devel-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-mls-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-targeted-3.13.1-23.el7_1.8.noarch.rpm, libipa_hbac-1.12.2-58.el7_1.14.s390x.rpm, libsss_idmap-1.12.2-58.el7_1.14.s390x.rpm, libsss_nss_idmap-1.12.2-58.el7_1.14.s390x.rpm, sssd-client-1.12.2-58.el7_1.14.s390x.rpm, sssd-common-1.12.2-58.el7_1.14.s390x.rpm, sssd-common-pac-1.12.2-58.el7_1.14.s390x.rpm, sssd-ipa-1.12.2-58.el7_1.14.s390x.rpm, sssd-krb5-common-1.12.2-58.el7_1.14.s390x.rpm, systemd-208-20.el7_1.5.s390x.rpm, systemd-libs-208-20.el7_1.5.s390x.rpm, systemd-sysv-208-20.el7_1.5.s390x.rpm, libgudev1-208-20.el7_1.5.s390x.rpm, trousers-0.3.11.2-4.el7_1.s390x.rpm, tzdata-2015e-1.el7.noarch.rpm, util-linux-2.23.2-22.el7_1.s390x.rpm, libblkid-2.23.2-22.el7_1.s390x.rpm, libmount-2.23.2-22.el7_1.s390x.rpm, libuuid-2.23.2-22.el7_1.s390x.rpm, wpa_supplicant-2.0-17.el7_1.s390x.rpm, dracut-fips-033-241.el7_1.3.s390x.rpm, dracut-fips-aesni-033-241.el7_1.3.s390x.rpm	see package names	Download

No	Type	Identifier	Release	Form of Delivery
8	SW (ppc64)	**Additional RPMs for ppc64** bind-libs-9.9.4-18.el7_1.2.ppc64.rpm, bind-libs-lite-9.9.4-18.el7_1.2.ppc64.rpm, bind-license-9.9.4-18.el7_1.2.noarch.rpm, bind-utils-9.9.4-18.el7_1.2.ppc64.rpm, binutils-2.23.52.0.1-30.el7_1.2.ppc64.rpm, ca-certificates-2015.2.4-70.0.el7_1.noarch.rpm, cups-1.6.3-17.el7_1.1.ppc64.rpm, cups-client-1.6.3-17.el7_1.1.ppc64.rpm, cups-filesystem-1.6.3-17.el7_1.1.noarch.rpm, cups-libs-1.6.3-17.el7_1.1.ppc64.rpm, device-mapper-1.02.93-3.el7_1.1.ppc64.rpm, device-mapper-event-1.02.93-3.el7_1.1.ppc64.rpm, device-mapper-event-libs-1.02.93-3.el7_1.1.ppc64.rpm, device-mapper-libs-1.02.93-3.el7_1.1.ppc64.rpm, lvm2-2.02.115-3.el7_1.1.ppc64.rpm, lvm2-libs-2.02.115-3.el7_1.1.ppc64.rpm, dnsmasq-2.66-13.el7_1.ppc64.rpm, dracut-033-241.el7_1.5.ppc64.rpm, dracut-config-rescue-033-241.el7_1.5.ppc64.rpm, dracut-network-033-241.el7_1.5.ppc64.rpm, freetype-2.4.11-10.el7_1.1.ppc64.rpm, glibc-2.17-79.el7_1.4.ppc64.rpm, glibc-common-2.17-79.el7_1.4.ppc64.rpm, gnutls-3.3.8-12.el7_1.1.ppc64.rpm, hwdata-0.252-7.8.el7_1.ppc64.rpm, iputils-20121221-6.el7_1.1.ppc64.rpm, kernel-3.10.0-229.26.2.el7.ppc64.rpm, kernel-headers-3.10.0-229.26.2.el7.ppc64.rpm, kernel-tools-3.10.0-229.26.2.el7.ppc64.rpm, kernel-tools-libs-3.10.0-229.26.2.el7.ppc64.rpm, kexec-tools-2.0.7-19.el7_1.2.ppc64.rpm, libgcrypt-1.5.3-12.el7_1.1.ppc64.rpm, libpcap-1.5.3-4.el7_1.2.ppc64.rpm, libreswan-3.12-10.1.el7_1.ppc64.rpm, libuser-0.60-7.el7_1.ppc64.rpm, libxml2-2.9.1-5.el7_1.2.ppc64.rpm, libxml2-python-2.9.1-5.el7_1.2.ppc64.rpm, nspr-4.10.8-2.el7_1.ppc64.rpm, nss-3.19.1-5.el7_1.ppc64.rpm, nss-sysinit-3.19.1-5.el7_1.ppc64.rpm, nss-tools-3.19.1-5.el7_1.ppc64.rpm, nss-util-3.19.1-5.el7_1.ppc64.rpm, nss-softokn-3.16.2.3-13.el7_1.ppc64.rpm, nss-softokn-freebl-3.16.2.3-13.el7_1.ppc64.rpm, openssh-6.6.1p1-12.el7_1.ppc64.rpm, openssh-clients-6.6.1p1-12.el7_1.ppc64.rpm, openssh-keycat-6.6.1p1-12.el7_1.ppc64.rpm, openssh-server-6.6.1p1-12.el7_1.ppc64.rpm, openssl-1.0.1e-42.el7_1.9.ppc64.rpm, openssl-libs-1.0.1e-42.el7_1.9.ppc64.rpm, python-2.7.5-18.el7_1.1.ppc64.rpm, python-libs-2.7.5-18.el7_1.1.ppc64.rpm, samba-libs-4.1.12-23.el7_1.ppc64.rpm, libwbclient-4.1.12-23.el7_1.ppc64.rpm, selinux-policy-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-devel-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-mls-3.13.1-23.el7_1.8.noarch.rpm, selinux-policy-targeted-3.13.1-23.el7_1.8.noarch.rpm, libipa_hbac-1.12.2-58.el7_1.14.ppc64.rpm, libsss_idmap-1.12.2-58.el7_1.14.ppc64.rpm, libsss_nss_idmap-1.12.2-58.el7_1.14.ppc64.rpm, sssd-client-1.12.2-58.el7_1.14.ppc64.rpm, sssd-common-1.12.2-58.el7_1.14.ppc64.rpm, sssd-common-pac-1.12.2-58.el7_1.14.ppc64.rpm, sssd-ipa-1.12.2-58.el7_1.14.ppc64.rpm, sssd-krb5-common-1.12.2-58.el7_1.14.ppc64.rpm, systemd-208-20.el7_1.5.ppc64.rpm, systemd-libs-208-20.el7_1.5.ppc64.rpm, systemd-sysv-208-20.el7_1.5.ppc64.rpm, libgudev1-208-20.el7_1.5.ppc64.rpm, trousers-0.3.11.2-4.el7_1.ppc64.rpm, tzdata-2015e-1.el7.noarch.rpm, util-linux-2.23.2-22.el7_1.ppc64.rpm, libblkid-2.23.2-22.el7_1.ppc64.rpm, libmount-2.23.2-22.el7_1.ppc64.rpm, libuuid-2.23.2-22.el7_1.ppc64.rpm, wpa_supplicant-2.0-17.el7_1.ppc64.rpm, dracut-fips-033-241.el7_1.3.ppc64.rpm, dracut-fips-aesni-033-241.el7_1.3.ppc64.rpm	see package names	Download

No	Type	Identifier	Release	Form of Delivery
9	SW (ppc64le)	**Additional RPMs for ppc64le** bind-libs-9.9.4-18.ael7b_1.2.ppc64le.rpm, bind-libs-lite-9.9.4-18.ael7b_1.2.ppc64le.rpm, bind-license-9.9.4-18.ael7b_1.2.noarch.rpm, bind-utils-9.9.4-18.ael7b_1.2.ppc64le.rpm, binutils-2.23.52.0.1-30.ael7b_1.2.ppc64le.rpm, ca-certificates-2015.2.4-70.0.ael7b_1.noarch.rpm, cups-1.6.3-17.ael7b_1.1.ppc64le.rpm, cups-client-1.6.3-17.ael7b_1.1.ppc64le.rpm, cups-filesystem-1.6.3-17.ael7b_1.1.noarch.rpm, cups-libs-1.6.3-17.ael7b_1.1.ppc64le.rpm, device-mapper-1.02.93-3.ael7b_1.1.ppc64le.rpm, device-mapper-event-1.02.93-3.ael7b_1.1.ppc64le.rpm, device-mapper-event-libs-1.02.93-3.ael7b_1.1.ppc64le.rpm, device-mapper-libs-1.02.93-3.ael7b_1.1.ppc64le.rpm, lvm2-2.02.115-3.ael7b_1.1.ppc64le.rpm, lvm2-libs-2.02.115-3.ael7b_1.1.ppc64le.rpm, dnsmasq-2.66-13.ael7b_1.ppc64le.rpm, dracut-033-241.ael7b_1.5.ppc64le.rpm, dracut-config-rescue-033-241.ael7b_1.5.ppc64le.rpm, dracut-network-033-241.ael7b_1.5.ppc64le.rpm, freetype-2.4.11-10.ael7b_1.1.ppc64le.rpm, glibc-2.17-79.ael7b_1.4.ppc64le.rpm, glibc-common-2.17-79.ael7b_1.4.ppc64le.rpm, gnutls-3.3.8-12.ael7b_1.1.ppc64le.rpm, hwdata-0.252-7.8.ael7b_1.ppc64le.rpm, iputils-20121221-6.ael7b_1.1.ppc64le.rpm, kernel-3.10.0-229.26.2.ael7b.ppc64le.rpm, kernel-headers-3.10.0-229.26.2.ael7b.ppc64le.rpm, kernel-tools-3.10.0-229.26.2.ael7b.ppc64le.rpm, kernel-tools-libs-3.10.0-229.26.2.ael7b.ppc64le.rpm, kexec-tools-2.0.7-19.ael7b_1.2.ppc64le.rpm, libgcrypt-1.5.3-12.ael7b_1.1.ppc64le.rpm, libpcap-1.5.3-4.ael7b_1.2.ppc64le.rpm, libreswan-3.12-10.1.ael7b_1.ppc64le.rpm, libuser-0.60-7.ael7b_1.ppc64le.rpm, libxml2-2.9.1-5.ael7b_1.2.ppc64le.rpm, libxml2-python-2.9.1-5.ael7b_1.2.ppc64le.rpm, nspr-4.10.8-2.ael7b_1.ppc64le.rpm, nss-3.19.1-5.ael7b_1.ppc64le.rpm, nss-sysinit-3.19.1-5.ael7b_1.ppc64le.rpm, nss-tools-3.19.1-5.ael7b_1.ppc64le.rpm, nss-util-3.19.1-5.ael7b_1.ppc64le.rpm, nss-softokn-3.16.2.3-13.ael7b_1.ppc64le.rpm, nss-softokn-freebl-3.16.2.3-13.ael7b_1.ppc64le.rpm, openssh-6.6.1p1-12.ael7b_1.ppc64le.rpm, openssh-clients-6.6.1p1-12.ael7b_1.ppc64le.rpm, openssh-keycat-6.6.1p1-12.ael7b_1.ppc64le.rpm, openssh-server-6.6.1p1-12.ael7b_1.ppc64le.rpm, openssl-1.0.1e-42.ael7b_1.9.ppc64le.rpm, openssl-libs-1.0.1e-42.ael7b_1.9.ppc64le.rpm, python-2.7.5-18.ael7b_1.1.ppc64le.rpm, python-libs-2.7.5-18.ael7b_1.1.ppc64le.rpm, samba-libs-4.1.12-23.ael7b_1.ppc64le.rpm, libwbclient-4.1.12-23.ael7b_1.ppc64le.rpm, selinux-policy-3.13.1-23.ael7b_1.8.noarch.rpm, selinux-policy-devel-3.13.1-23.ael7b_1.8.noarch.rpm, selinux-policy-mls-3.13.1-23.ael7b_1.8.noarch.rpm, selinux-policy-targeted-3.13.1-23.ael7b_1.8.noarch.rpm, libipa_hbac-1.12.2-58.ael7b_1.14.ppc64le.rpm, libsss_idmap-1.12.2-58.ael7b_1.14.ppc64le.rpm, libsss_nss_idmap-1.12.2-58.ael7b_1.14.ppc64le.rpm, sssd-client-1.12.2-58.ael7b_1.14.ppc64le.rpm, sssd-common-1.12.2-58.ael7b_1.14.ppc64le.rpm, sssd-common-pac-1.12.2-58.ael7b_1.14.ppc64le.rpm, sssd-ipa-1.12.2-58.ael7b_1.14.ppc64le.rpm, sssd-krb5-common-1.12.2-58.ael7b_1.14.ppc64le.rpm, systemd-208-20.ael7b_1.5.ppc64le.rpm, systemd-libs-208-20.ael7b_1.5.ppc64le.rpm, systemd-sysv-208-20.ael7b_1.5.ppc64le.rpm, libgudev1-208-20.ael7b_1.5.ppc64le.rpm, trousers-0.3.11.2-4.ael7b_1.ppc64le.rpm, tzdata-2015e-1.ael7b.noarch.rpm, util-linux-2.23.2-22.ael7b_1.ppc64le.rpm, libblkid-2.23.2-22.ael7b_1.ppc64le.rpm, libmount-2.23.2-22.ael7b_1.ppc64le.rpm, libuuid-2.23.2-22.ael7b_1.ppc64le.rpm, wpa_supplicant-2.0-17.ael7b_1.ppc64le.rpm	see package names	Download

Table 2: Deliverables of the TOE

2.1. Overview of Delivery Procedure

The TOE is delivered from the developer, Red Hat, using the Red Hat delivery mechanism described below . There are several download components: the Red Hat Enterprise Linux Server 7.1 distribution (ISO file) files, and additional packages created specifically for the evaluation of RHEL 7.1 (containing the kickstart file, Evaluated Configuration Guide, and configuration files), and multiple additional packages that must be installed to obtain the TOE. The packages and ISO files are delivered via the same delivery mechanism.

RHEL 7.1 is delivered via the Red Hat Network (RHN), an online retrieval system provided by the developer. The packages are built by the Red Hat Release Engineering Group and immediately signed using the Red Hat PGP private Key (the public key is widely distributed and available). ISO images are created and SHA-256 checksums of the images are generated. The ISO images for the release are transferred to a staging area on the web server hosting the RHN using SSH. The SHA-256 checksums for the images are verified to ensure that the image has not been modified. The image is then moved to the public download area and the SHA-256 checksum is checked again to verify that the image has not been modified. Customers download the ISO images and are advised within the [10] to verify the checksums and the signatures.

The package download is securely provided by the developer, reviewed and built into an RPM, signed by Release Engineering using the signing key referenced above, and electronically delivered by Red Hat's distribution network. Customers who download the package are advised to verify the signature.

2.2. Identification of the TOE by the User

The customer can identify the TOE packages in the download sites by appropriate labeling. The download page lists the release and the architecture (for example "Red Hat Enterprise Linux Server for (v. 7.1 for x86_64)"). The downloaded ISO image is named according to release and architecture like in rhel-server-7.1-<platform>-dvd.iso. Following installation, the user can verify by looking at the content of file /etc/release that the installed version is "Red Hat Enterprise Linux Server release 7.1". The evaluated configuration is achieved, when the user follows the instructions provided in [10], which is part of the "cc-config-rhel71-*.rpm" packages.

For all packages, the user can verify their integrity by downloading the RedHat signing key from the download website and running the rpm --checksig command as described in the Evaluated Configuration Guide. To verify whether the correct versions of the packages have been installed, users can use the rpm -qa command and search the output for the respective packages.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Auditing
- Cryptographic support
- Packet filter
- Identification and Authentication
- Discretionary Access Control (DAC)

- Mandatory Access Control (MAC)
- Security Management
- Runtime Protection Mechanisms
- Linux Container Framework Support (not on POWER architecture)

For more details please refer to Table 1 and the Security Target [6], chapter 7.3.

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:

- competent and trustworthy administrators
- trusted remote IT systems
- procedures for information protection
- installation and configuration in a secure manner
- careful system maintenance
- physical protection
- secure recovery mechanisms

Details can be found in the Security Target [6], chapter 6.1.

5. Architectural Information

The TOE is structured in much the same way as many other operating systems, especially Unix-type operating systems. It consists of a kernel, which runs in the privileged state of the processor and provides services to applications (which can be used by calling kernel services via the system call interface). Direct access to the hardware is restricted to the kernel, so whenever an application wants to access hardware like disk drives, network interfaces or other peripheral devices, it has to call kernel services. The kernel then checks if the application has the required access rights and privileges and either performs the service or rejects the request.

The kernel is also responsible for separating the different user processes. This is done by the management of the virtual and real memory of the TOE which ensures that processes executing with different attributes cannot directly access memory areas of other processes but have to do so using the inter-process communication mechanism provided by the kernel as part of its system call interface.

The TSF of the TOE also include a set of trusted processes, which when initiated by a user, operate with extended privileges. The programs that represent those trusted processes on the file system are protected by the file system discretionary access control security function enforced by the kernel.

In addition, the execution of the TOE is controlled by a set of configuration files, which are also called the TSF database. Those configuration files are also protected by the file system discretionary access control security function enforced by the kernel.

Normal users – after they have been successfully authenticated by a defined trusted process – can start untrusted applications where the kernel enforces the security policy of the TOE when those applications request services from the kernel via the system call interface.

The TOE includes a secure system initialization function which brings the TOE into a secure state after it is powered on or after a reset. This function ensures that user interaction with the TOE can only occur after the TOE is securely initialized and in a secure state.

6. Documentation

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

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

7. IT Product Testing

7.1. Developer Testing

All the hardware plattforms which are outlined in chapter 8 have been tested.

The developer did not test all machines of all families, but at least one machine for each CPU and virtualization type as the other differences between the machines are related to the provided hardware environment that has no impact on the security of the TOE.

Developer Testing Approach

The test plan provided by the developer lists test cases by groups, which reflects the mix of sources for the test cases. The provided mapping lists the SFRs and the TSFI the test cases are associated with. The test plan is focused on the security functions of the TOE and ignores other aspects typically found in developer test plans. The test cases are mapped to the corresponding functional specification and HLD.

The developer uses one test suite which pulls in tests from older test suites (LTP) for some specific cases, but the actual handling of this is transparent to the user. The test suite has a common framework for the automated tests in which individual test cases adhere to a common structure for setup, execution and cleanup of tests. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behavior with illegal parameters and reaction to missing privileges). Each test within a test case reports PASS, OK or FAIL and the test case summary in batch mode reports PASS if all the tests within the test case passed, otherwise FAIL. All the tests were executed successfully (pass).

Developer Testing Results

The test results provided by the developer were generated on the hardware platform listed above. As described in the testing approach, the test results of all the automated tests are written to files.

All test results from all tested environments show that the expected test results are identical to the actual test results.

Developer Test Coverage

The functional specification has identified the following different TSFI:

- system calls (which applies to most other resource like files, IPC, network socket)
- security critical configuration files (TSF databases)
- trusted programs and the corresponding network protocol (SSH v2, TLS, and IPsec) or program-specific local protocols (DBus)

The mapping provided by the developer shows that the tests cover all individual TSFI identified for the TOE. An extension to this mapping developed by the evaluator as documented in the test case coverage analysis document shows that also significant details of the TSFI have been tested with the developer's test suite.

Developer Test Depth

In addition to the mapping to the functional specification, the developer provided a mapping of test cases to subsystems of the TOE design and the internal interfaces described in the TOE design at subsystem level. This mapping shows that all subsystems and the internal interfaces are covered by test cases. To show evidence that the internal interfaces have been called, the developer provided the description of the internal interfaces as part of the TOE design. The interfaces are clear enough to allow the evaluator to assess whether they have been covered by testing.

Not all of the internal interfaces mentioned in the TOE design at subsystem level could be covered by direct test cases. Due to the restrictions of the evaluated configuration, some internal interfaces can only be invoked during system startup. This especially includes internal interfaces to load and unload kernel modules, to register / de-register device drivers and install / de-install interrupt handlers. Since the evaluated configuration does not allow to dynamically load and unload device drivers as kernel modules, those interfaces are only used during system startup and are, therefore, implicitly tested there.

7.2. Evaluator Testing Effort

The evaluator verified the test systems according to the documentation in the Evaluated Configuration Guide [10] and the test plan. The test setup for the independent testing consisted of developer test systems only (accessed remotely), and the configuration contained both Base and MLS systems. Also one system including a dm-crypt setup was used.

The evaluator testing effort consisted of two parts. The first one was the execution of the developer tests and the second one was the execution of the tests created by the evaluator. The evaluator did not rerun all tests on all machines, but a reasonable sample size with a focus on 64bit as this is the typical usage for the TOE to gain confidence in the developer tests. Therefore not all permutations where run.

In addition to repeating the tests that were provided by the developer according to the test plan from the developer, the evaluator decided to run some additional test cases on the provided test systems:

- Permission settings of relevant configuration files
- Capability test
- Netlink restrictions
- Verification of code vulnerability protection functions:

    - return address modification on the stack
    - program section overwrite
    - kernel code execution in user space
- NSS protocol tests
- OpenSSL and NSS timing tests
- additional dm-crypt cipher tests
- SSH cipher tests
- IPsec tests (ciphers and certificates)

All tests passed.

Evaluator Penetration Testing

The following parts of the TOE were scheduled for testing:

1. "Seccomp Filtering" (Not present on POWER architecture)
2. "Stack Canaries can be guessed"
3. "DBus fuzzing"
4. "OpenSSH authentication"
5. "syscall thrashing"
6. "CVE-2015-5157"
7. Virtual filesystem permissions

The evaluator chose a mix of source code based assessment, fuzzing of complex interfaces as well as directed testing of possible flaws to identify flaws within the TOE.

The TOE was in its evaluated configuration, as indicated in AVA_VAN.3-1: Application level tests ran on a virtualized x86 platform, system call level tests ran on the actual platforms (x86, s390, ppc64 and ppc64le) and source code level tests were made using an editor.

The evaluator chose a mix of kernel level (system calls) and application level interfaces (DBus, OpenSSH, virtual filesystems) covering authentication and authorization to perform penetration testing.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration is documented in the Evaluated Configuration Guide [10]. It is based on Red Hat Enterprise Linux 7.1 (RHEL 7.1) with additional packages as listed in Table 2.The software may be used on the following hardware platforms specified in the Security Target [6]:

- HP based on x86 64bit Intel Xeon processors:
    - HP ProLiant ML series G7, Gen8, Gen9 product line
    - HP ProLiant DL series G7, Gen8, Gen9 product line
    - HP ProLiant BL series G7, Gen8, Gen9 product line
    - HP ProLiant SL series G7, Gen8, Gen9 product line

- HP based on AMD64 processors:
  - HP ProLiant ML series G7, Gen8 product line
  - HP ProLiant DL series G7, Gen8 product line
  - HP ProLiant BL series G7, Gen8 product line
  - HP ProLiant SL series G7, Gen8 product line
- Dell based on x86 64bit Intel:
  - Dell PowerEdge R920
  - Dell PowerEdge R930
  - Dell PowerEdge T430, T630, R430, R530, R630, R730, R730xd, M630, M830, FC430, FC630, FC830, C6320, and Precision R7910
- IBM System p based on Power 8 processors providing execution environments with PowerVM:
  - Big Endian with PowerVM: Tuleta BE model number - Power 835 model 8286-41A
  - Little Endian with RHEV for Power 3.6: Power 835 model 8284-22A
- IBM System z based on z/Architecture processors:
  - zEnterprise EC12 (zEC12)
  - zEnterprise BC12 (zBC12)
  - zEnterprise 196 (z196)
  - zEnterprise 114 (z114)

The following virtual environment has also been tested:

- KVM on x86 hardware as provided by RHEL 7 or later
- KVM on POWER LE hardware as provided by RHEV-H 3.6 or later

This Evaluated Configuration Guide specifies a number of constraints, such as configuration values for various configuration files, specific steps to be taken during installation and information to administrators on how to manage the TOE.

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used.

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

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_FLR.3 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0754-2012, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on linux containers, current version of upstream packages pulled, boot sequence, enhanced audit, modified hardware.

The evaluation has confirmed:

- PP Conformance: Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010, OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010 [8]
- for the Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.3

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).

Cryptographic statement SSH

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
1	Authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-1 (ssh-rsa)	[RFC3447], PKCS#1 v2.1 sec.8.2 (RSA) [FIPS180-4] (SHA) [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	Modulus length: 1024, 2048, 3072 and 4096	no	Public keys are exchanged trustworthily out of band, e.g. checking fingerprints.

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
2	Authentication	DSA signature generation and verification using SHA-1 (ssh-dss)	[FIPS186-4] (DSA) [FIPS180-4] (SHA) [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	plength = 1024 (L) qlength = 160 (N)	no	
3	Authentication	ECDSA signature generation and verification using SHA-{256, 384, 512} on nistp-{256, 384, 521} (ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521)	[ANSI X9.62] (ECDSA), [FIPS180-4] (SHA), NIST curves [FIPS186-4] identifiers analogous to [RFC5903], sec 5 [RFC5656] secp{256,384,521}r1 [SEC2] [RFC4253] (SSH-TRANS) for host authentication [RFC4252], sec. 7 (SSH-AUTH) for user authentication	plength = 256, 384, 521 depends on selected curve	yes	
4	Authentication	User name and password-based authentication	[RFC4252], sec. 5 (SSH-AUTH) for user authentication	Guess success prob. $\varepsilon \leq 2^{-20}$	no	PAM is used centrally. Thus if the authentication is aborted the counter for failed logins is increased and remains as is for the next login. (FIA_SOS.1)
5	Key agreement (key exchange)	DH with DH group1-sha1	[RFC4253] (SSH-TRANS) supported by [RFC2409] (DH groups IKE) [FIPS-180-4] (SHA)	plength = 1024	no	
6	Key agreement (key exchange)	DH with DH group14-sha1	[RFC4253] (SSH-TRANS) supported by [RFC3526] (DH groups IKE) [FIPS-180-4] (SHA)	plength = 2048	yes	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
7	Key agreement (key exchange)	DH with diffie-hellman-group-exchange-{sha1, sha256}	[RFC4253] (SSH-TRANS) supported by [RFC4419] (DH-Group Exchange) [FIPS-180-4] (SHA)	plength = 1024, 1536	no	As of /etc/ssh/moduli
				Plength = 2048, 3072, 4096	yes	
8	Key agreement (key exchange)	ECDH with ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521 (ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521)	[RFC4253] (SSH-TRANS) [FIPS-180-4] (SHA) supported by [RFC5656] (ECC in SSH) secp{256,384,521}r1 [SEC2] NIST curves [FIPS186-4] identifiers analogous to [RFC5903], sec 5	plength = 256, 384, 521 depends on selected curve	yes	
9	Confidentiality	Three-key TDES in CBC mode (3des-cbc)	[SP 800-67] (TDES/TDEA), [SP 800-38A] (CBC), [RFC4253] (SSH-TRANS using 3DES with CBC mode)	|k|=168	yes	Binary packet protocol (BPP): encryption
10	Confidentiality	AES in CBC mode, and CTR mode (aes128-cbc, aes192-cbc, aes256-cbc) (aes128-ctr, aes192-ctr, aes256-ctr);	[FIPS197] (AES), [SP 800-38A] (CBC), [RFC 4253] (SSH-TRANS using AES with CBC mode), [RFC4344] (SSH-2 using AES with CTR mode)	|k|=128, 192, 256	yes	
11	Integrity and Authenticity	HMAC-SHA-1 (hmac-sha1)	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC2404] (HMAC using truncated SHA-1) [RFC4251] / [RFC4253] (SSH HMAC support) [RFC6668] (SHA-2 in SSH)	|k|= 160	yes	BPP: Message authentication

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
12	Integrity and Authenticity	HMAC-SHA-2 (hmac-sha2-256, hmac-sha2-512)	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support) [RFC6668] (SHA-2 in SSH)	|k|= 256, 512	yes	BPP: Message authentication
13	Authenticated encryption (encrypt-then authenticate)	HMAC-SHA-1 (hmac-sha1-etm@openssh.com) HMAC-SHA-2 (hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com) + CBC-AES	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support), [RFC6668] (SHA-2 in SSH)	|k|=160, 256, 512	yes	etm = encrypt-then-MAC (OpenSSH 6.2)
14	Authenticated encryption	AES in GCM mode (aes128-gcm@openssh.com, aes256-gcm@openssh.com)	[RFC5647]	|k|=128, 256	yes	
15	Key generation	RSA key generation with key size: 1024, 2048, 3072, 4096 bits	[FIPS 186-4], B.3.3 and C.3 for Miller Rabin primality tests.	n/a	n/a	Host keys and user keys Using either FCS_RNG.1 (SSL-DFLT) in non-FIPS mode or (SSL-FIPS) in FIPS mode
16	Key generation	DSA key generation with key size: {L=1024, N=160},	[FIPS 186-4], B.1	n/a	n/a	
17	Key generation	ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS 186-4], B.4	n/a	n/a	
18	Trusted channel	FTP_ITC.1 a) ST [6], sec. 6.2.1.50 for SSHv2.0	Cf. all lines above,	See above	yes / no	Depending on the security level of the used mechanisms above.

Table 3: Cryptographic functionality of SSH implemented within the TOE

Cryptographic Statement TLS

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
1	Authenticity Server certificate validation	RSA signature verification (RSASSA-PKCS1-v1_5) using SHA-1	[FIPS186-4] (RSA) referring to [RFC3447] (PKCS#1 v2.1) [FIPS180-4] (SHA)	Modulus length: 1024, 2048, 3072, 4096	no	Verification of certificate signatures provided for authentication of the server at the client side. Server certificates are always required,
2	Authenticity	RSA signature verification	[RFC3447] (PKCS#1	Modulus length:	no	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
		(RSASSA-PKCS1-v1_5) using SHA-256, SHA-384, SHA-512	v2.1) [FIPS180-4] (SHA)	1024		client certificates optional. Algorithms used depending on the signature algorithm / hash algorithm used for signing the certificates and the accepted signature algorithms / hash algorithms by the server. The certificates / keys may be generated by the TOE or imported into the TOE. Please refer to [6] in FCS_CKM.1 and [10].
				Modulus length: 2048, 3072 4096	yes	
3	Authenticity	DSA signature verification using SHA-1	[FIPS186-4] (DSA) [FIPS180-4] (SHA)	L=1024, N=160 L= 2048, N= 224 / 256 L=3072, N=256	no	
4	Authenticity	DSA signature verification using SHA-256, SHA-384, SHA-512	[FIPS186-4] (DSA) [FIPS180-4] (SHA)	L=1024, N=160	no	
				L= 2048, N= 224 / 256 L=3072, N=256	yes	
5	Authenticity	ECDSA signature generation and verification using SHA-1 on NIST P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), EC: secp{256, 384, 521}r1 [SEC2]; P-{256, 384, 521} [FIPS186-4]	Key sizes corresponding to the used elliptic curve plength = 256, 384, 521	no	Only NIST curves NIST P-256, NIST P-384, or NIST P-521 are allowed – see [10].
6	Authenticity	ECDSA signature generation and verification using SHA-256, SHA-384, SHA-512 on NIST P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), EC: P-{256, 384, 521} [FIPS186-4]	plength ≥ 250 e.g for the curves: NIST-curve P-{256, 384, 521} ([FIPS186-4])	yes	
7	Authentication Client Depending on the server's certificate request and client's certificate	RSA signature generation (client) (RSASSA-PKCS1-v1_5[8]) using SHA-1	[RFC3447] (PKCS#1 v2.1) [RFC5246] (TLSv1.2)	Modulus length: 1024, 2048, 3072, 4096	no	CertificateVerify: Client provides signature over the whole handshake message. This message is only sent following a client certificate that has signing capability (i.e., all certificates except those containing fixed DH
8	Authentication	RSA signature generation (client)	[RFC3447] (PKCS#1 v2.1)	Modulus length: 1024	no	

[8] Implicitly EMSA-PKCS1-v1_5 encoding method is required based on block type 1 (PS = FF).

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
		(RSASSA-PKCS1-v1_5) using SHA-256, SHA-384, SHA-512	[RFC5246] (TLSv1.2)	Modulus length: 2048, 3072 4096	yes	parameters)
9	Authentication	RSA signature generation (client). (RSASSA-PKCS1-v1_5) using MD5 / SHA-1 combination.	[RFC3447] (PKCS#1 v2.1) [RFC4346](TLSv1.1)	Modulus length: 1024, 2048, 3072 4096	no	
10	Authentication	DSA signature verification using SHA-1	[FIPS186-4] (DSA) [FIPS180-4] (SHA)	L=1024, N=160 L= 2048, N= 224 / 256 L=3072, N=256	no	
11	Authentication	DSA signature verification using SHA-256, SHA-384, SHA-512	[FIPS186-4] (DSA) [FIPS180-4] (SHA)	L=1024, N=160	no	
				L= 2048, N= 224 / 256 L=3072, N=256	yes	
12	Authentication	ECDSA signature generation using SHA-1 on NIST P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), EC: P-{256, 384, 521} [FIPS186-4]	Key sizes corresponding to the used elliptic curve plength = 256, 384, 521	no	Client cert Type: ecdsa_sign. The public key of the certificate MUST use a curve and point format supported by the server.
13	Authentication	ECDSA signature generation and verification using SHA-256, SHA-384, SHA-512 on NIST P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), EC: P-{256, 384, 521} [FIPS186-4]	Key sizes corresponding to the used elliptic curve plength = 256, 384, 521	yes	
14	Authentication	DSA signature verification using SHA-1 *(TLS_DHE_DSS)*	[FIPS186-4] (DSA) [FIPS180-4] (SHA) [RFC5246] (TLSv1.2) [RFC4346] (TLSv1.1)	L=1024, N=160 L= 2048, N= 224 / 256 L=3072, N=256	no	
15	Authentication	DSA signature verification using SHA-256, SHA-384 *(TLS_DHE_DSS)*	[FIPS186-4] (DSA) [FIPS180-4] (SHA) [RFC5246] (TLSv1.2) [RFC4346] (TLSv1.1)	L=1024, N=160	no	
				L= 2048, N= 224 / 256 L=3072, N=256	yes	
16	Authentication	RSA signature verification (RSASSA-PKCS1-v1_5) using SHA-1	[RFC3447] (PKCS#1 v2.1) [FIPS180-4] (SHA)	modulus length: 1024, 2048, 3072, 4096	no	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
		(TLS_DHE_RSA, TLS_ECDHE_RSA)	[RFC5246] (TLSv1.2)			
17	Authentication	RSA signature verification (RSASSA-PKCS1-v1_5) using SHA-256, SHA-384 *(TLS_DHE_RSA, TLS_ECDHE_RSA)*	[RFC3447] (PKCS#1 v2.1) [FIPS180-4] (SHA) [RFC5246] (TLSv1.2)	modulus length: 1024	no	
				modulus length: 2048, 3072 4096	yes	
18	Authentication	RSA signature verification (RSASSA-PKCS1-v1_5) using MD5 / SHA-1 combination	[RFC3447] (PKCS#1 v2.1) [RFC4346] (TLSv1.1)	modulus length: 1024, 2048, 3072 4096	no	For TLS 1.1
19	Authentication	ECDSA signature verification using SHA-1 on NIST P-256, P-384 and P-521 *(TLS_ECDHE_ECDSA)*	[ANSI X9.62] (ECDSA), [FIPS180-4] (SHA), [RFC4492] (ECC for TLS)	Key sizes corresponding to the used elliptic curve plength = 256, 384, 521	no	
20	Authentication	ECDSA signature verification using SHA-256, SHA-384, SHA-512 on NIST P-256, P-384 and P-521 *(TLS_ECDHE_ECDSA)*	[ANSI X9.62] (ECDSA), [FIPS180-4] (SHA), [RFC4492] (ECC for TLS),	Key sizes corresponding to the used elliptic curve plength = 256, 384, 521	yes	
21	Key establishment: Key transport	RSA encryption (client) (RSAES-PKCS1-v1_5[9]) *(TLS_RSA)*	[RFC3447] (PKCS#1 v2.1) [SP800-56B] (IFC key establishment)	modulus length: 1024	no	Server certificate is used for key exchange.
				modulus length: 2048, 3072 4096	yes	
22	Key establishment: Key agreement Ephemeral	DHE MODP groups: exponentiation groups modulo a prime	[RFC5246]	≧ 2048	yes	Only DH-groups equal or larger than 2048 bit are allowed, see [10].
23	Key establishment: Key agreement	ECDHE ECP groups: elliptic curve	[RFC4492] (ECC for TLS)	Key sizes corresponding to	yes	Only NIST curves NIST P-256, NIST

[9] Implicitly EME-PKCS1-v1_5 encoding method is required based on block type 2 (PS= random data).

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
	Ephemeral	groups over GF[P] NIST P-256, P-384 and P-521	[TR-03111] (ECC) [SP800-56-A] (ECC DH) [FIPS186-4] (EC: P-{256, 384, 521})	the used elliptic curve plength = 256, 384, 521		P-384, or NIST P-521 are allowed – see [10].
24	Key derivation	PRF: HMAC with SHA-256, 384 (default: prf_sha256 for TLSv1.2, also prf_sha384 possible)	[FIPS198-1] (HMAC) [FIPS180-4] (SHA) [RFC5246](TLSv1.2)	variable	yes	Symmetric keys and MAC keys for record layer.
25	Key derivation	PRF: HMAC with MD5 and SHA-1 in combination (default: prf for TLS v1.0, v1.1)	[FIPS198-1] (HMAC) [RFC1321], RFC6151] (MD5) [FIPS180-4] (SHA) [RFC2246] (TLS v1.0) [RFC4346] (TLS v1.1)	variable	yes	
26	Confidentiality	AES in CBC mode *(AES_128_CBC, AES_256_CBC)*	[FIPS197] (AES) [SP800-38A] (CBC)	|k|=128, 256	yes	Bulk data encryption / decryption (record layer)
27	Confidentiality	Three-key TDES in CBC mode *(3DES_EDE_CBC)*	[SP 800-67] (TDES/TDEA), [SP 800-38A] (CBC), [RFC4253] (SSH-TRANS using 3DES with CBC mode)	|k|=168	yes	
28	Authenticated Encryption	AES in GCM mode *(AES_128_GCM, AES_256_GCM)*	[FIPS197] (AES) [RFC5228] (AES GCM within TLS)	|k|=128, 256	yes	
29	Integrity and authenticity	HMAC with SHA-1 or SHA-256 or SHA-384 *(SHA), (SHA256), (SHA384)*	[FIPS198-1] (HMAC) [FIPS180-4] (SHA)	160 (SHA-1) 256 (SHA-256) 384(SHA-384)	yes	Message authentication code (record layer)
30	Key generation	RSA key generation with key sizes: 1024, 2048, 3072, 4096 bits	[FIPS186-4], B.3.3 and C.3 for Miller Rabin primality tests.	n/a	n/a	Keys for certificates and for certificate signing, using FCS_RNG.1(NSS).
31	Key generation	DSA key generation with key sizes: {L=1024, N=160 bits}; {L=2048, N=224 bits}; {L=2048, N=256 bits}; {L=3072, N=256 bits};	[FIPS186-4], B.1	n/a	n/a	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
32	Key generation	ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS186-4], B.4	n/a	n/a	
33	Trusted Channel	FTP_ITC.1 [ST], sec. 6.2.1.50 b)	Cf. all lines above	See above	yes	Depending on the sec. level of the used mechanisms above.
					no	

Table 4: Cryptographic functionality of TLS implemented within the TOE

Cryptographic statement IPsec / IKE

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
1	Authenticity	RSA signature verification (RSASSA-PKCS1-v1.5) using SHA-1	[RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 1024, 2048, 3072 and 4096	no	Algorithms used depending on the signature algorithm / hash functions used for signing the certificates
2	Authenticity	RSA signature verification (RSASSA-PKCS1-v1.5) using SHA-256, SHA-384, SHA-512	[RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 1024	no	
				Modulus length: 2048, 3072 and 4096	yes	
3	Authenticity	DSA signature verification using SHA-1	[FIPS186-4] (DSA) [FIPS180-4] (SHA)	L=1024, N=160 L= 2048, N= 224 / 256 L=3072, N=256	no	
4	Authenticity	DSA signature verification using SHA-256, SHA-384, SHA-512	[FIPS186-4] (DSA) [FIPS180-4] (SHA)	L=1024, N=160	no	
				L= 2048, N= 224 / 256 L=3072, N=256	yes	
5	Authenticity	ECDSA signature verification using SHA-1 on NIST P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), EC: secp{256, 384, 521}r1 [SEC2]	Key sizes correspondin g to the used elliptic curve plength = 256, 384, 521	no	Only NIST curves NIST P-256, NIST P-384, or NIST P-521 are allowed – see [10].
6	Authenticity	ECDSA signature verification using SHA-256, SHA-384, SHA-512 on NIST P-256, P-384 and P-521	[FIPS186-4] (ECDSA),	Key sizes correspond-ing to the	yes	Recommendati on use for signatures of certificates:

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
			[FIPS180-4] (SHA), EC: secp{256, 384, 521}r1 [SEC2]	used elliptic curve plength = 256, 384, 521		SHA-256 on P-256 curve SHA-384 on P-384 curve SHA-512 on P-521 curve if any.
7	IKE authentication	RSAES-PKCS1-v1_5 encryption scheme with private key encryption for signing and public key decryption for signature verification. (Auth Method 1)	[RFC2409] (IKEv1), [RFC3447] (RSA)	Modulus length: 1024	no	HASH_I and HASH_R are encrypted. The values are derived using the PRF.
				Modulus length: 2048, 3072 and 4096	yes	
8	IKE authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-1 (Auth Method 1)	[5996] (IKEv2) [RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 1024, 2048, 3072 and 4096	no	
9	IKE authentication	RSA signature generation and verification RSASSA-PKCS1-v1.5 using SHA-256, SHA-384, SHA-512 (Auth Method 1)	analogous to [RFC7427] [RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 1024	no	
				Modulus length 2048, 3072 and 4096	yes	
10	IKE key agreement	DH with DH groups based on FFC:	[RFC2409] (IKEv1), [RFC5996] (IKEv2) [DH] (DH as referenced in [RFC2409] & [RFC5996])			
11	IKE key agreement	MODP groups: exponentiation groups modulo a prime	[RFC2409] group 2 1024-bit MODP group	plength= 1024	no	
12	IKE key agreement	MODP groups: exponentiation groups modulo a prime	[RFC3526] group 5 1536-bit MODP group	plength= 1536	no	
13	IKE key agreement	MODP groups: exponentiation groups modulo a prime	[RFC3526] groups 14, 15, 16, 17,18 (2048, 3072, 4096, 6144, 8192)-bit MODP groups	plength= 2048, 3072, 4096, 6144, 8192	yes	
14	IKE key agreement	MODP groups: exponentiation groups modulo a prime	[RFC5114] group 22 1024-bit MODP group with 160-bit prime order subgroups	plength= 1024	no	
15	IKE key agreement	MODP groups: exponentiation groups modulo a prime	[RFC5114] groups 23, 24 2048-bit MODP	plength= 2048	yes	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
			group with (224, 256)-bit prime order subgroups			
16	IKE key derivation	PRF based on: HMAC-SHA1 (ID 2 PRF_HMAC_SHA1) HMAC with SHA-256 (ID 5 PRF_HMAC_SHA2_256) HMAC with SHA-384 (ID 6 PRF_HMAC_SHA2_384) HMAC with SHA-512 (ID 7 PRF_HMAC_SHA2_512)	[RFC5996] (IKEv2), [RFC2409] (IKEv1), [FIPS198-1] (HMAC), [FIPS180-4] (SHA) [RFC4868] (HMAC -SHA2 with IPsec) [IKEV2IANA]	|k| = variable[10]	yes	IKE keys (IKE SA) and IPsec keys (IPsec SA / child SA) are derived according to the key length required for the negotiated algorithms they are used for[11]
17	IKE integrity and authenticity and IPsec ESP integrity and authenticity	HMAC with SHA-1-96 (ID 2 AUTH_HMAC_SHA1_96)	[RFC 5996], [RFC4307] (IKEv2) [RFC2409] (IKEv1) [FIPS180-4] (SHA), [FIPS198-1] (HMAC), [RFC2404] (HMAC using truncated SHA-1) [IKEV2IANA] [RFC4595] (HMAC-SHA-1)	|k|=160, 256, 384, 512	yes	
18	IKE encryption and IPsec ESP encryption	AES in CBC mode (ID 12 ENCR_AES_CBC)	[RFC5996] (IKEv2) [RFC2409] (IKEv1) [RFC3602] supported by [RFC4307]	|k|=128, 192, 256	yes	
19	IKE encryption and IPsec ESP encryption	AES in CTR mode (ID 13 ENCR_AES_CTR)	[RFC5930], [RFC3686] supported by [RFC4307]	|k|=128, 192, 256	yes	
20	IKE encryption and IPsec ESP encryption	TDES in CBC mode i.e. 3DES-EDE-CBC (ID 3 ENCR_3DES)	[RFC5996], [RFC2451] supported by [RFC4307]	|k|=168	yes	Triple-DES shall not be used for encrypting more than 2^32 64-bit data blocks.

[10] preferred key size = size of the output of the underlying hash function

[11] Note that for IKEv1 [RFC2409] in general the PRF (pseudo-random function) and hash is negotiated separately, not as within IKEv2 where the whole PRF is negotiated. If the PRF is not negotiated the HMAC version of the negotiated Hash is used as PRF.

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
21	Key generation	RSA key generation with key sizes: 1024, 2048, 3072, 4096 bits	[FIPS186-4], B.3.3 and C.3 for Miller Rabin primality tests.	n/a	n/a	Keys for certificates and for certificate signing, using FCS_RNG.1 (NSS).
22	Key generation	DSA key generation with key sizes: {L=1024, N=160 bits}; {L=2048, N=224 bits}; {L=2048, N=256 bits}; {L=3072, N=256 bits};	[FIPS186-4], B.1	n/a	n/a	
23	Key generation	ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS186-4], B.4	n/a	n/a	
24	Trusted Channel	FTP_ITC.1 b), [6] sec. 6.2.1.47 for IKEv2, IPsec ESP	Cf. all lines above, especially [RFC5996] (IKEv2) [RFC4303] (ESP)	See above	yes no	Depending on the sec. level of the used mechanisms above Either in transport mode or in tunnel mode

Table 5: Cryptographic functionality of IPsec (IKEv1 / IKEv2 and ESP) implemented within the TOE

Cryptographic statement LUKS-based dm-crypt

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
1	Key derivation with authentication (access control, protection / recovery mode)	Password based key derivation using PBKDF2 with PRF HMAC using SHA-1, SHA-256, SHA-384, SHA-512	[SP800-132] [CFLUKS][12] [RFC2898] (PBKDF2) [FIPS198-1] (HMAC), [FIPS180-4] (SHA)	Guessing prob. 2^{-20} Salt 32 byte iteration count 1000 ms	no	
2	Confidentiality (bulk data & key access / key wrapping)	AES in CBC mode IV-handling mechanism: CBC-ESSIV (SHA-1, SHA-256, SHA-384, SHA-512)	[FIPS197] (AES) [SP800-38A] (CBC)	|k| = 128, 192, 256	yes	
3	Confidentiality (bulk data & key access / key wrapping)	AES in XTS mode IV-handling mechanism: XTS-plain64 XTS-benbi	[FIPS197] [SP800-38E] (XTS)	|k|= 2*128, 2*192, 2*256	yes	

Table 6: Cryptographic functionality for LUKS-based dm-crypt Linux partition implemented within the TOE

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.

[12] Please note that the master key of [CFLUKS] is called DPK in [SP800-132]. And in [SP800-132] the Master key is called the key which is derived from the user password.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

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

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[13] 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] Red Hat Enterprise Linux, Version 7.1 Security Target, Version 0.21, Date 2016-06-09, Red Hat, Inc.

[7] Evaluation Technical Report, Version: 3, Date: 2016-06-30, atsec information security GmbH (confidential document)

[8] Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010, OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010

[9] Configuration list for the TOE: CI list for source, Date 2016-05-13, File name rhel-71-brew-logs.tar.bz2 (confidential document)

[10] EAL4 Evaluated Configuration Guide for Red Hat Enterprise Linux 7.1, Version 0.25, Date 2016-06-09

[13] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

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.