Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0962-2016

for

SUSE Linux Enterprise Server Version 12

from

SUSE LLC

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0962-2016 (*)

Operating System

SUSE Linux Enterprise Server
Version 12

from	SUSE LLC
PP Conformance:	Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Packages: Advanced Management, Advanced Audit, and Virtualization all Version 2.0, 28 May 2010
Functionality:	PP conformant 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, 24 February 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 SUSE Linux Enterprise Server, Version 12 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0852-2013. Specific results from the evaluation process BSI-DSZ-CC-0852-2013 were re-used.

The evaluation of the product SUSE Linux Enterprise Server, Version 12 was conducted by atsec information security GmbH. The evaluation was completed on 19 February 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: SUSE LLC.

The product was developed by: SUSE LLC.

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

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 24 February 2016 is valid until 23 February 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 Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,

[6] Information Technology Security Evaluation Facility

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

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

5. Publication

The product SUSE Linux Enterprise Server, Version 12 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] SUSE LLC
1800 South Novell Place
Provo, UT 84606
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 SUSE Linux Enterprise Server 12, a highly-configurable Linux-based operating system.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, and three OSPP Extended Packages [8]:

- Advanced Management, Version 2.0, 28 May 2010,
- Advanced Audit, Version 2.0, 28 May 2010,
- Virtualization, Version 2.0, 28 May 2010

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 6.2. 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. The TOE can be deployed as an audit server that receives audit logs from other TOEinstances.
Cryptographic support	The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. In addition, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt.
Packet filter	The TOE provides a stateless and stateful packet filter for regular IP-based communication.
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.
Discretionary Access Control	DAC allows owners of named objects to control the access permissions to these objects.
Authoritative Access Control	The TOE supports authoritative or mandatory access control
Virtual machine environments	The TOE implements the host system for virtual machines.
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.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.5.2.2.

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:

SUSE Linux Enterprise Server, Version 12

The following table outlines the TOE deliverables:

No	Identifier	Type	Form of Delivery
1	SLE-12-Server-DVD-x86_64-CC-Respin-A-DVD1.iso (SHA256: cd13e6fef73f5d9c7718f8938bd60e141447868e36da312faf3fb36cceb06b3b)	ISO	D/L
2	SLE-12-Server-DVD-x86_64-CC-Respin-A-DVD2.iso (SHA256: 18300cd26cae108f7e87449a6111452cb74a0df7ed1fb3ea4968c979978ca7e7)	ISO	D/L
3	SLE-12-Server-DVD-x86_64-CC-Respin-A-DVD3.iso (SHA256: b172adf4f874dbf9b1cc7b2d66fa5104e9f4d75dd4fb5b61477a9e8fb8b45ace)	ISO	D/L
4	SLE-12-Server-DVD-s390x-CC-Respin-A-DVD1.iso (SHA256: 006ef29887a1bbabdbd87ea766d5525058161f3bc9bb569894f4955b1f9bbb61)	ISO	D/L
5	SLE-12-Server-DVD-s390x-CC-Respin-A-DVD2.iso (SHA256: 5094b2c977cadf50139d2a09c0486f3c3a5a6c900227e9669a27defc17268178)	ISO	D/L
6	SLE-12-Server-DVD-s390x-CC-Respin-A-DVD3.iso (SHA256: cf7a7fedad3d6c1b4a41f2c93e584dacc0dc7725eaaef466a35f99f9d95f600c)	ISO	D/L
7	certification-sles-eal4-12.0-0.16.1.noarch.rpm (SHA256: 6f140298480da65471b8c11e9d0b2ed8fa146dc4b63640bfb2f96beb63de4809) RPM contains the "Evaluated Configuration Guide" [10] This is the version for x86_64 and it is available at: https://download.suse.com/Download?buildid=vfg4TGVmOvs%7e	RPM	D/L
8	certification-sles-eal4-12.0-0.16.1.noarch.rpm (SHA256: 5db4eb0a11a46360a56a4dc478cf32953fed85511cab0d1e2a36eb6edca87444) RPM contains the "Evaluated Configuration Guide" [10] This is the version for s390x and it is available at: https://download.suse.com/Download?buildid=FdQP4afr8G0%7e	RPM	D/L

Table 2: Deliverables of the TOE

The delivery of the TOE is electronic download only in the form of DVD ISO images according to the ECG [10]. The TOE's downloadable parts are shown in Scope of TOE

Supply (section 2). The packages the make up the TOE are digitally signed using GPG. The key of the developer is contained on the installation DVD, as described in the ECG.

The developer provides and operates the download site and provides checksums for the downloaded images that enable the user to verify the integrity of the download. In addition this certification report provides SHA256 checksums in table 2 for aditional integrity verification.

The ECG is a central document to the evaluation. It defines how to install and configure the TOE. It is being shipped as part of a signed RPM package and is thus integrity protected as well.

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, Authoritative Access Control, Virtual machine environments and Security Management.

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:

- Those responsible for the TOE are competent and trustworthy
- If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected.
- Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner (e.g. network cabling, DAC protections on security-relevant files, etc.).
- Those responsible for the TOE must ensure that the system is installed and configured in a secure manner.
- Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
- Those responsible for the TOE must ensure that the TOE is protected from physical attacks.
- Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
- Those responsible for the TOE must ensure that remote trusted IT systems are under the same management domain as the TOE.
- The trusted IT systems executing the TOE supports the enforcement of the security policy.

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

5. Architectural Information

SLES is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications. In addition, virtual machines provide an execution environment for a large number of different operating systems.

The SELinux LSM is configured to enforce the authoritative access control policy. The following access control rules are enforced by enabled LSM:

Isolation of virtual machines from each other by assigning each process implementing a virtual machine and its resources a unique label. Access between virtual machines and resources is only permitted if the label of the virtual machine and the accessed resource is identical.

The SLES evaluation covers a potentially distributed network of systems running the evaluated versions and configurations of SLES as well as other peer systems operating within the same management domain. The hardware platforms selected for the evaluation consist of machines which are available when the evaluation has completed and to remain available for a substantial period of time afterwards.

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

The hardware, the BIOS firmware and potentially other firmware layers between the hardware and the TOE are considered to be part of the TOE environment.

The TOE includes standard networking applications, including applications allowing access of the TOE via cryptographically protected communication channels, such as SSH.

System administration tools include the standard command line tools. A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a network server using a port above 1024 may be used as a normal application running without root privileges on top of the TOE. The additional documentation specific for the evaluated configuration provides guidance how to set up such applications on the TOE in a secure way.

5.1. TOE Structure and Security Functions

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

The kernel is also responsible for separating the different user processes. This is done by the management of the virtual and real memory of the TOE which ensures that processes

executing with different attributes cannot directly access memory areas of other processes but have to do so using the inter-process communication mechanism provided by the kernel as part of its system call interface.

The TSF of the TOE also 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.

The kernel acts as a hypervisor for the virtual machine support of the TOE. It uses the virtualization support of the underlying processor to provide virtual machines with the required kernel support in KVM and user space support via libvirt.

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.

The TOE provides the following security functionality:

Auditing

The Lightweight Audit Framework is designed to be an audit system making Linux compliant with the requirements from Common Criteria. Lightweight Audit Framework is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem allows configuring the events to be actually audited from the set of all events that are possible to be audited.

The TOE can be deployed as an audit server that receives audit logs from other TOE instances. These audit logs are stored locally. The TOE provides search and review facilities to authorized administrators for all audit logs.

Cryptographic support

The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. For interactive usage, the SSHv2 protocol is provided. The TOE provides the server side as well as the client side applications. Using OpenSSH, password-based and public-key-based authentication are allowed.

In addition to OpenSSH, the TOE provides IPSec for a cryptographically secured communication with other remote entities. IPSec is offered together with IKEv2 for the key negotiating aspect. The implementations of IKEv2 allow a pre-shared key or certificate based authentication of the remote peer.

In addition, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt. Using this device mapper target, the Linux operating system offers administrators and users cryptographically protected block device storage space.

With the help of a Password-Based Key-Derivation Function version 2 (PBKDF2) implemented with the LUKS mechanism, a user-provided passphrase protects the volume key which is the symmetric key for encrypting and decrypting data stored on disk. Any data

stored on the block devices protected by dm_crypt is encrypted and cannot be decrypted unless the volume key for the block device is decrypted with the passphrase processed by PBKDF2. With the device mapper mechanism, the TOE allows for transparent encryption and decryption of data stored on block devices, such as hard disks.

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.

The packet filtering functionality offered by the TOE is hooked into the TCP/IP stack of the kernel at different locations. Based on these locations, different filtering capabilities are applicable. The lower level protocols are covered by the EBTables filter mechanism which includes the filtering of Ethernet frames including the ARP layer. The higher level protocols of TCP/IP are covered with the IPTables mechanism which allows filtering of IP and TCP, UDP, ICMP packets. In addition, IPTables offers a stateful packet filter for the mentioned higher level protocols.

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. The authentication security function allows password-based authentication. For SSH access, public-key-based authentication is also supported. Password quality enforcement mechanisms are offered by the TOE which are enforced at the time when the password is changed.

Discretionary Access Control

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. In addition to the standard Unix-type permission bits for file system objects as well as IPC objects, the TOE implements POSIX access control lists. These ACLs allow the specification of the access to individual file system objects down to the granularity of a single user.

Authoritative Access Control

The TOE supports authoritative or mandatory access control based on the following concept:

To separate virtual machines and their resources at runtime SELinux rules are used. The virtual machine resources are labeled to belong to one particular virtual machine. In addition a virtual machine is awarded a unique label. The TOE ensures that virtual machines can only access resources bearing the same label.

Virtual machine environments

The TOE implements the host system for virtual machines. It acts as a hypervisor which provides an environment to allow other operating systems execute concurrently. SELinux labels are attached to virtual machines and its resources. The access control policy is

enforced using these labels to grant virtual machines access to resources if the category of the virtual machine is identical to the label of the accessed resource.

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. Status.

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. Test Configuration

The developer provided the following test systems to run the independent tests on:

IBM System z (zEC12), AMD 64bit (x3755) and Intel 64bit (x3650).

For the actual evaluation testing on the hardware specified in ST [6] and (ECG) [10], the test systems provided by the developer which were accessed remotely via SSH were used. He also used a KVM hypervisor on an test machine in the ITSEF lab to prepare the evaluator tests.

On these systems the evaluator verified the compliance with ST [6] and ECG [10] by checking the installed configuration for the actual use of the appropriate settings that the AutoYaST file provides before the start of the tests.

The evaluator also checked the installed packages on the test system to verify that only the packages that are required according to the ECG [10] and the developer test plan are installed.

The examination of the test system confirmed that the test system are compliant with the setup instructions from the ECG [10] which have been analyzed as a direct implementation of the ST in the guidance work units.

To determine the consistency of the test environment with the ST [6], the evaluator also reviewed the objectives for the operational environment. The evaluator did not identify any objective that is relevant to the test environment. All of the objectives ensure that the TOE is installed and operated in a secured environment by competent personnel which is considered to be given for the test environment. Besides, the test system does not contain any user or TSF data which needs to be protected.

The evaluator verified that the hardware configuration required by the ST [6] is provided by the developer. The evaluator identified that all the requirements of the ST [6] are fulfilled including the assumptions made in the ST [6].

7.2. Developer Testing

The evaluator examined the information provided by the developer and determined the following:

Test configuration

The test results provided by the developer were generated on the following systems:

Intel x86_64 architecture and IBM s390x (z architecture)

The developer has performed his tests on the above listed hardware platform. The software was installed and configured as defined in the ECG [10] with additional software packages identified in the Test Plan. Each of the test result files contains a logfile that documents the installed configuration that was in effect for the test tun.

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 the subsystems.

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. In addition, several tests although originating from the automated test suite have to be executed manually. 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.

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. The results of the manual tests have also been documented in a separate file.

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

Test coverage

The functional specification has identified the following different TSFI:

- System Calls
- Trusted programs (and the corresponding network protocol SSH v2.)
- KVM IOCTLs and hypervisor calls
- TSF database files (security critical configuration files)
- SELinux interfaces including its configuration and control files
- DBUS Programs
- socket protocols (e.g. netlink)
- general network protocols applicable to information flow control
- IPsec

- Miscellaneous interfaces that don't fit into the categories above, either because there are no external interfaces, or the security functionality is not directly visible at the interface.

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.

Test depth

In addition to the mapping to the functional specification, the developer provided a mapping of test cases to subsystems of the high-level design and the internal interfaces described in the high-level design. 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 high-level 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 high-level design could be covered by direct test cases. Some internal interfaces can – due to the restrictions of the evaluated configuration – only be invoked during system startup. This includes especially 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.

Conclusion

The evaluator has verified that developer testing was performed on hardware conformant to the ST [6].

The evaluator was able to follow and fully understand the developer testing approach by using the provided test documentation. The evaluator analyzed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem/internal interfaces identified in the hight level design.

The evaluator reviewed the test results provided by the developer and found them to be consistent with the expected test results according to the test plan.

7.3. Evaluator Testing Effort

When performing independent evaluator tests, the evaluator determined the following:

TOE test configuration

The evaluator verified the test systems according to the documentation in the Evaluated Configuration Guide [10] and the test plan. As assessed in the evaluation report on the administrator guidance, the ECG is consistent with the ST. Hence, the evaluator concludes that the evaluator's configuration is consistent with the ST.

The evaluator performed tests on all hardware architectures types supported in the evaluation.

Evaluator tests performed

In addition to running all the automated developer tests, the evaluator devised tests for a subset of the TOE.The evaluator has chosen these tests for the following reasons:

- a variation of an audit-test case to verify the result checking in the test framework works as expected
- a variation of an audit-test case to verify the file system object DAC tests on different file systems (the developer tests normally only use one file system type), to ensure that DAC is enforced as expected (with a few known exception as some file systems do not support some file object types).
- some basic privilege checks for some management commands that can only be performed by root
- functionality provided through the netlink interface and which requires certain commands to be only to be executed by root
- an additional test of the dbus access controls for existing policyKit rules
- a variation of the IPsec cipher tests as this protocol is new in the evaluation scope
- IPsec certificate tests to extend the IPsec tests of the developer
- additional SSH cipher tests to extend the test scope of the developer

The evaluator created several test cases for testing a few functional aspects where the developer test cases were considered by the evaluator to be not broad enough.

Summary of Evaluator test results

The evaluator testing effort consists of two parts. The first one is the execution of the developer tests and the second is the execution of the tests created by the evaluator.

The tests were performed remotely at the developer's or the developer's data center depending on the desired test system. The systems available for testing are listed above.

In each case the system was accessible through SSH. The TOE operating system with the required tools were installed on the test machine by the developer according to the instructions in ECG [10], and which were verified by the evaluator. The configuration scripts triggered by the AutoYaST installation ensured the evaluation-compliant system configuration. After running the automated configuration, no further system configuration was performed and only the tools required for testing where installed. The test systems were therefore configured according to the ST and the instructions in the ECG. The evaluator verified the configuration against the ECG before conducting the independent tests. The log files generated by the test cases were analyzed for completeness and failures. The developer provided automated test cases.

All the test results conformed to the expected test results from the test plan. 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.

All developer and evaluator tests were successful.

Evaluator Penetration Testing

The following parts of the TOE were scheduled for testing:

- libvirtd's handling of labels
- DBus fuzzing

- OpenSSH authentication
- syscall thrashing
- CVE-2015-5157

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

The TOE was in its evaluated configuration. Application level tests ran on a Virtual Box platform, system call level tests ran on the actual platforms and source code level tests were made using an editor.

8. Evaluated Configuration

This certification covers the following configurations of the TOE. It defines a number of hardware platforms in [6], section 1.4.4:

- x86 64bit Intel Xeon processors: HP ProLiant BL460c G1
- x86 64bit AMD Opteron processors: HP ProLiant BL465c G1
- IBM based on System z:
  - zEnterprise EC12 (zEC12)
  - zEnterprise BC12 (zBC12)
  - zEnterprise 196 (z196)
  - zEnterprise 114 (z114)

The installation of the TOE must be carried out as described in [10], which describes the actual installation steps as well as additional configuration steps that need to be carried out when the TOE is installed.

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used. For RNG assessment the scheme 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-0852-2013, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on KVM support for IBM

System Z, the RNG implementation, the file system BTRFS, changes in Systemd and the Dbus/Polkit.

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 – Advanced Audit, Version 2.0, 28 May 2010,
  OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3

The TOE partly consists of open source software. It is common to share flaw information in its community.

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).

SSH

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
0	Authentication	The client authenticates either with UserID & password (#5) or by cryptographic means as shown in #1-#4 and verified by the server respectively.				
1		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	Modulus length: 1024, 2048, 3072 and 4096	no	Pubkeys are exchanged trustworthily out of band, e.g. checking fingerprints. Authenticity is not part of the TOE. (no certificates are used)

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
			[RFC4252], sec. 7 (SSH-AUTH) for user authentication			
2		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		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		User name and password-based authentication	[RFC4252], sec. 5 (SSH-AUTH) for user authentication	Guess success prob. $\varepsilon \leq 2^{-20}$	yes	PAM is used centrally. Thus if the authentication is aborted the counter for failed logins is increased and remains as is for the next login.
5	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
6		DH with diffie-hellman-group-exchange-{sha1, sha256}	[RFC4253] (SSH-TRANS) supported by [RFC4419] (DH-Group Exchange) [FIPS-180-4] (SHA)	plength=1024	no	As of /etc/ssh/moduli
				plength= 2K, 3K, 4K, etc.	yes	
7		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	
8	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
9		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	
10	Integrity and Authenticity	HMAC-SHA-2 (hmac-sha2-256, hmac-sha2-512)	[FIPS180-4] (SHA) [RFC2104] (HMAC), [RFC4251] / [RFC4253] (SSH HMAC support)	|k|= 256, 512	yes	BPP: Message authenti-cation
11	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)
12		AES in GCM mode (aes128-gcm@openssh.com, aes256-gcm@openssh.com)	[RFC5647]	|k|=128, 256	yes	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comment
13	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
14		DSA key generation with key size: {L=1024, N=160},	[FIPS 186-4], B.1	n/a	n/a	
15		ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS 186-4], B.4	n/a	n/a	
16	Trusted channel	FTP_ITC.1 a) [ST], sec. 6.2.1.47 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

Please note that for key derivation the same hash function as used for key agreement is used in order to generate IVs, encryption keys and integrity keys from the shared secret and the exchanged hash. This is done for each direction client-to-server and server-to client.

IPsec

Please note that KEv2 RFC5996 is obsoleted by RFC7296 and updated by RFC7427 in the meantime. However, the TOE is still implemented as stated in the ST [6] according to RFC5996.

#	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	Verification of certificate signatures provided for authenti-cation Server and client certificates are used. Algorithms used depending on the signature algorithm* / hash functions** used for signing the certificates
2		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:	yes	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
				2048, 3072 and 4096		
3		ECDSA signature verification using SHA-1 on P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-3] (SHA), EC secp{256, 384, 521}r1 [SEC2]	Key sizes corres-pondin 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 [ECG]. Recommen-dati on use for signatures of certificates: SHA-256 on P-256 curve SHA-384 on P-384 curve SHA-521 on P-521 curve if any.
4		ECDSA signature verification using SHA-256, SHA-384, SHA-512 on P-256, P-384 and P-521	[FIPS186-4] (ECDSA), [FIPS180-3] (SHA), EC secp{256, 384, 521}r1 [SEC2]	Key sizes corres-pondin g to the used elliptic curve plength =256, 384, 521	yes	
5	IKE authentication	RSA signature generation and verification (Auth Method 1) RSASSA-PKCS1-v1.5 using SHA-1	[5996] (IKEv2) [RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 1024, 2048, 3072 and 4096	no	
6		RSA signature generation and verification (Auth Method 1) RSASSA-PKCS1-v1.5 using SHA-256, SHA-384, SHA-512	analogous to [RFC7427] [RFC3447] (RSA) [FIPS180-4] (SHA)	Modulus length: 1024	no	
				Modulus length 2048, 3072 and 4096	yes	
7		ECDSA signature generation and verification with SHA-256 on P-256 curve SHA-384 on P-384 curve SHA-521 on P-521 curve (Auth Method 9, 10, 11)	[FIPS 186-4] [FIPS180-4](SHA) [RFC4754] (IKEv2 using ECDSA), EC secp{256, 384, 521}r1 [SEC2]	Key sizes corresponding to the used elliptic curve plength =256, 384, 521	yes	
8	IKE key agreement	DH with DH groups based on FFC and ECC	[RFC5996] (IKEv2), [DH] (DH as referenced in [RFC5996])			
9		MODP groups: exponentiation groups modulo a prime	[RFC2409] group 2 1024-bit MODP group	plength= 1024	no**	
10			[RFC3526] group 5	plength= 1536	no**	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
			1536-bit MODP group			
11			[RFC3526] groups 14, 15, 16, 17,18 (2048, 3072, 4096, 6144, 8192)-bit MODP groups	plength= 2048, 3072, 4096, 6144, 8192	yes	
12			[RFC5114] group 22 1024-bit MODP group with 160-bit prime order subgroups	plength= 1024	no**	
13			[RFC5114] groups 23, 24 2048-bit MODP group with (224, 256)-bit prime order subgroups	plength= 2048	yes	
14		ECP groups: elliptic curve groups over GF[P]	NIST curves [FIPS186-4] identifiers analogous to [RFC5903], sec 5			
15			[RFC5114] group 19: 256-bit random ECP group (secp256r1[SEC2])	plength=256	yes	
16			[RFC5114] group 20: 384-bit Random ECP Group (secp384r1[SEC2])	plength=384	yes	
17			[RFC5114] group 21: 521-bit Random ECP Group (secp521r1[SEC2])	plength=521	yes	
18			[RFC5114] group 25: 192-bit Random ECP group (secp192r1[SEC2])	plength= 192	no	
19			[RFC5114] group 26, 224-bit Random ECP group (secp224r1[SEC2])	plength= 224	yes*	
20		ECP groups: elliptic curve groups over GF[P]	Brainpool curves [RFC5639]			
21			[RFC6954] group 27 brainpoolP224r1	plength= 224	yes*	
22			[RFC6954] group 28, 29, 30	plength= 256, 384, 521	yes	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
			elliptic curve brainpoolP{256, 384, 512}r1			
23	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), [FIPS198-1] (HMAC), [FIPS180-4] (SHA) [RFC4868] (HMAC -SHA2 with IPsec) [IKEV2IANA]	|k| = variable[8]	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[9]
24	IKE integrity and authenticity and IPsec ESP integrity and authenticity	HMAC with SHA1 (ID7 AUTH_HMAC_SHA1_160) HMAC with SHA-1-96 (ID 2 AUTH_HMAC_SHA1_96) HMAC with SHA-256-128 (ID 12 AUTH_HMAC_SHA2_256_128) HMAC with SHA-384-192 (ID 13 AUTH_HMAC_SHA2_384_192) HMAC with SHA-512-256 (ID 14 AUTH_HMAC_SHA2_512_256)	[RFC 5996], [RFC4307] (IKEv2) [FIPS180-4] (SHA), [FIPS198-1] (HMAC), [RFC4868] (HMAC -SHA2 with IPsec) [RFC2404] (HMAC using truncated SHA-1) [IKEV2IANA] [RFC4595] (HMAC-SHA-1)	|k|=160, 256, 384, 512	yes	
25	IKE encryption and IPsec ESP encryption	AES in CBC mode (ID 12 ENCR_AES_CBC)	[RFC5996], [RFC3602] supported by [RFC4307]	|k|=128, 192, 256	yes	
26		AES in CTR mode (ID 13 ENCR_AES_CTR)	[RFC5930], [RFC3686] supported by [RFC4307]	|k|=128, 192, 256	yes	
27		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.
28	IKE authenticated	AES in CCM mode	[RFC5282],	|k|=128, 192,	no	AEAD

[8] preferred key size = size of the output of the underlying hash function / key size of AES = 128 bit

[9] Note that for IKEv2 the whole PRF is negotiated not as within IKEv1 where the hash is negotiated separately.

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
	encryption and IPsec ESP authenticated encryption	(ID 14 ENCR_AES-CCM_8)	[RFC4309], [RFC5116]	256		
29		AES in CCM mode (ID 15 ENCR_AES-CCM_12) (ID 16 ENCR_AES-CCM_16)	[RFC5282], [RFC4309], [RFC5116]	|k|=128, 192, 256	yes	
30		AES in GCM mode (ID 18 AES-GCM with a 8 octet ICV)	[RFC5282], [RFC4106], [RFC5116]	|k|=128, 192, 256	no	
31		AES in GCM mode (ID 19 AES-GCM with a 12 octet ICV) (ID 20 AES-GCM with a 16 octet ICV)	[RFC5282], [RFC4106], [RFC5116]	|k|=128, 192, 256	yes	
32	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	Keys for certificates and for certificate signing Using either FCS_RNG.1 (SSL-DFLT) in non-FIPS mode or (SSL-FIPS) in FIPS mode
33		ECDSA key generation based on NIST curves: P-256, P-384 and P-521	[FIPS 186-4], B.4	n/a	n/a	
34	Trusted Channel	FTP_ITC.1 b), [ST] 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 4: Cryptographic functionality of IPsec (IKEv2 and ESP) implemented within the TOE

dm-crypt based on LUKS

#	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] [RFC2898] (PBKDF2) [FIPS198-1] (HMAC) [FIPS180-4](SHA)	Guessing prob. 2^{-20} Salt 32 byte iteration count 1000 ms	yes	
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] [SP800-38A] (CBC)	|k|= 128,192,256,	yes	
3		AES in XTS mode IV-handling mechanism: XTS-plain64 XTS-benbi	[FIPS197] [SP800-38E] (XTS)	|k|= 2*128, 2*192, 2*256	yes	

Table 5: 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.

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
ACL	Access Control List
API	Application Programming Interface
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
ECG	Evaluated Configuration Guide
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KVM	Kernel Virtualized Machine
LUKS	Linux Unified Key Setup
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
VPN	Virtual Private Network

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.

DAC - Discretionary Access Control implemented with permission bits and ACLs.

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.

IOMMU - Input / Output Memory Management Unit. This MMU allows the setup of multiple DMA areas for different virtual machines.

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

PAM - Pluggable Authentication Module - the authentication functionality provided with Linux is highly configurable by selecting and combining different modules implementing different aspects of the authentication process.

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.

SELinux - Linux kernel LSM module that is able to implement arbitrary security policies. An SELinux policy distributed with the TOE implements multi-level or multi-category security.

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[10] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0962-2016, Version 2.10 Date 2016-02-12, Security Target for SUSE Linux Enterprise Server 12 including KVM virtualization, SUSE and atsec

[7] Evaluation Technical Report, Version 3, Date 2016-02-18, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Packagses Advanced Management, Advanced Audit, Virtualization, all Version 2.0, 28 May 2010

[9] Configuration lists for the TOE, Version n/a, Date 2016-02-18, MASTER CM List, File name “sles12-cmlist-master-v1.zip”, (confidential document)

[10] Guidance documentation for the TOE, Version 1.14, Date February 17, 2016, Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server 12 (ECG)

[11] [FIPS180-4] Federal information processing standards (FIPS), Secure Hash Standard (SHS), March 2012

[12] [FIPS186-4] Federal information processing standards (FIPS), Digital Signature Standard , July 2013

[13] [FIPS197] Federal information processing standards (FIPS), Advanced Encryption Standard, November 2001

[14] [FIPS198-1] Federal information processing standards (FIPS), The Keyed-Hash Message Authentication Code (HMAC), July 2008

[10] specifically

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

[15] [IEEEP1619] IEEE P1619™/D16, Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, May 2007

[16] [IKEV2IANA] "Internet Key Exchange Version 2 (IKEv2) Parameters", https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xml

[17] [PKCS#1v2.1] RSA Laboratories, PKCS #1: RSA Cryptography Standard, Version 2.1, dated June 14, 2002

[18] [RFC2404] The Use of HMAC-SHA-1-96 within ESP and AH, C. Madson, R. Glenn, 1998-11-01

[19] [RFC2409] The Internet Key Exchange (IKE), D. Harkins, D. Carrel, 1998-11-01

[20] [RFC3280] Internet X.509 Public Key Infrastructure CertiAcate and CertiAcate Revocation List (CRL) ProAle, R. Housley, W. Polk, W. Ford, D. Solo, April 2002

[21] [RFC3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography SpeciAcations, Version 2.1, J. Jonsson, B. Kaliski, 2003-02-01

[22] [RFC3526] More Modular Exponential (MODP) DiQe-Hellman groups for Internet Key Exchange (IKE), T. Kivinen, M. Kojo, 2003-05-01

[23] [RFC4109] Algorithms for Internet Key Exchange version 1 (IKEv1), P. HoDman, 2005-05-01

[24] [RFC4251] The Secure Shell (SSH) Protocol Architecture, T. Ylonen, C. Lonvick, 2006-01-01

[25] [RFC4252] The Secure Shell (SSH) Authentication Protocol, T. Ylonen, C. Lonvick, Ed., 2006-01-01

[26] [RFC4253] The Secure Shell (SSH) Transport Layer Protocol, T. Ylonen, C. Lonvick, 2006-01-01

[27] [RFC4301] Security Architecture for the Internet Protocol, S. Kent, K. Seo, December 2005

[28] [RFC4303] IP Encapsulating Security Payload (ESP), S. Kent, December 2005

[29] [RFC4304] Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP), S. Kent, December 2005

[30] [RFC4344] The Secure Shell (SSH) Transport Layer Encryption Modes , M. Bellare, T. Kohno, C. Namprempre, 2006-01-01

[31] [RFC4868] Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, S. Kelly, S. Frankel, 2007-05-01

[32] [RFC5077] Transport Layer Security (TLS) Session Resumption without Server-Side State, J. Salowey, H. Zhou, P. Eronen, H. Tschofenig, January 2008,

[33] [RFC5280] Internet X.509 Public Key Infrastructure CertiAcate and CertiAcate Revocation List (CRL) ProAle, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, May 2008

[34] [RFC5282] Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, D. Black, D. McGrew, August 2008

[35] [RFC5647] AES Galois Counter Mode for the Secure Shell Transport Layer Protocol, August 2009, http://tools.ietf.org/html/rfc5647

[36] [RFC5996] Internet Key Exchange Protocol Version 2 (IKEv2), C. Kaufman, P. HoDman, Y. Nir, P. Eronen, 2010-09-01

[37] [RFC6989] Additional DiQe-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2), Y. SheDer, S. Fluhrer, July 2013

[38] [SP800-38A-Add] National Institute of Standards and Technology. SP800-38AAddendum: Rec- ommendation for Block Cipher Modes of Operation: Three Variants of Cipher- text Stealing for CBC Mode. 2010.

[39] [SP800-38A] National Institute of Standards and Technology. SP800-38A: Recommendation for Block Cipher Modes of Operation. 2001.

[40] [SP800-38B] National Institute of Standards and Technology. SP800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. 2005.

[41] [SP800-38C] National Institute of Standards and Technology. SP800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and ConAdentiality. 2004.

[42] [SP800-38D] National Institute of Standards and Technology. SP800-38A: Recommenda- tion for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. 2007.

[43] [SP800-38E] National Institute of Standards and Technology. SP800-38E: Recommendation for Block Cipher Modes of Operation: The XTSAES

[44] Mode for ConAdentiality on Storage Devices. 2010. [SP800-67] National Institute of Standards and Technology. SP800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Version 1.1, May 19, 2008

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.