Certification Report

BSI-DSZ-CC-0754-2012

for

**Red Hat Enterprise Linux,
Version 6.2 with KVM Virtualization for x86
Architectures**

from

Red Hat, Inc.

Deutsches IT-Sicherheitszertifikat

erteilt vom · Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0754-2012

Operating System

Red Hat Enterprise Linux
Version 6.2 with KVM Virtualization for x86 Architectures

from	Red Hat, Inc.
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 – Labeled Security, Version 2.0, 28 May 2010, OSPP Extended Package – Virtualization, 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

Common Criteria
Recognition
Arrangement

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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 23 October 2012
For the Federal Office for Information Security

Bernd Kowalski   L.S.
Head of Department

SOGIS
IT SECURITY CERTIFIED

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:

● BSIG[2]

● BSI Certification Ordinance[3]

● BSI Schedule of Costs[4]

● Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)

● DIN EN 45011 standard

● BSI certification: Procedural Description (BSI 7125) [3]

● Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]

● Common Methodology for IT Security Evaluation, Version 3.1 [2]

● 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

As of September 2011 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.Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2   International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

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 6.2 with KVM Virtualization for x86 Architectures has undergone the certification procedure at BSI.

The evaluation of the product Red Hat Enterprise Linux, Version 6.2 with KVM Virtualization for x86 Architectures was conducted by atsec information security GmbH. The evaluation was completed on 10 September 2012. The 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, Inc..

The product was developed by:Red Hat, Inc..

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

4   Validity of the Certification Result

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

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,

---

[6]   Information Technology Security Evaluation Facility

● 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.

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.

5   Publication

The product Red Hat Enterprise Linux, Version 6.2 with KVM Virtualization for x86 Architectures 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, Inc.
      Varsity Drive
      NC 27506 Raleigh
      USA

This page is intentionally left blank.

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 TOE is Red Hat Enterprise Linux, Version 6.2 with KVM Virtualization for x86 Architectures with security patches.

Red Hat Enterprise Linux (RHEL) 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 [7] together with the following extended packages specified for the OSPP:

● Extended package for Advanced Management (MLS mode only)

● Extended package for Audit

● Extended package for Labeled Security (MLS mode only)

● Extended package for Virtualization

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 adds 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 except the extended package of labeled security as well as advanced management. SELinux must be enabled if the administrator wants to provide virtual machines.

In MLS mode the SELinux security module is configured to enforce the authorative access control policy based on the labels of subjects and objects as required by the extended package for labeled security as well as advanced management. Note that a system in MLS mode can optionally be configured to use a single sensitivity label for all subjects and objects to provide an operational mode equivalent to pure role-based access control specified in the OSPP extended package for advanced management with no mandatory access control.

RHEL provides a virtualization environment based on the Linux KVM technology. RHEL implements the host system for the virtual machine environment and manages the virtual machines. In addition, RHEL provides management interfaces to administer the virtual machine environment as well as full auditing of user and administrator operations.

The KVM technology separates the runtime environment of virtual machines from each other. The Linux kernel operates as the hypervisor to the virtual machines but provides a normal computing environment to administrators of the virtual machines. Therefore, the Linux kernel supports the concurrent execution of virtual machines and regular applications. RHEL uses the processor virtualization support to ensure that the virtual machines execute close to the native speed of the hardware.

In addition to the separation of the runtime environment, RHEL also provides system-inherent separation mechanisms to the resources of virtual machines. This separation ensures that the large software component used for virtualizing and simulating devices executing for each virtual machine cannot interfere with each other. Using the SELinux multi-category mechanism, the virtualization and simulation software instances are isolated. The virtual machine management framework configures SELinux multi-category settings transparently to the administrator.

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 – Advanced Audit, Version 2.0, 28 May 2010,
OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010,
OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010 [7].

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 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functions	Addressed issue
Auditing	The Lightweight Audit Framework (LAF) is designed to be an audit system making Linux compliant with the requirements from OSPP. LAF 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.
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. In addition, the access to the virtual machine administration tool as well as the virtual machine consoles can be protected using an SSHv2-based tunnel.
Packet filter	The TOE provides a stateless and stateful packet filter for regular IP-based communication. Layer 3 (IP) and 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.
Confidentiality-protected data storage	Using dm_crypt, the Linux operating system offers administrators and users cryptographically protected block device storage space. Only with the passphrase can the encryption key used for encryption or decryption be obtained and used. Any data stored on the block devices protected by dm_crypt is encrypted and cannot be accessed even when the TOE is not operational unless the TOE is operational and the block device session key is unlocked.
Authoritative Access	The TOE supports mandatory access control based on the following concepts:

TOE Security Functions	Addressed issue

Control	• Sensitivity labels which are automatically attached to processes and objects. The access control policy enforced using these labels is derived from the Bell-LaPadula access control model.
	
	 • SELinux categories are attached to virtual machines and their resources. The access control policy enforced using these categories grant virtual machines access to resources if the category of the virtual machine is identical to the category of the accessed resource.
	
	 • Role-based access control is implemented with roles that are defined via types and access to types. A "type" is a security attribute given to an object or a process. The type of a process is commonly called a "domain". Policy rules define how domains may interact with objects and with other domains. Roles can be assigned to users and define which user can have access to which domain. A user may have several roles assigned to him but will always act in one role only. To change from his current role to another role that has been assigned to the user, the TOE provides an application which requires re-authentication. The TOE has a hierarchical set of roles defined in the policy. Those are:
	
	   • Root administrator: This is the classical superuser role which is hierarchical to all other roles,
	
	   • System process: This is a role that should be assigned to specific system processes like daemons,
	
	   • System administrator: This is a role for general system administration,
	
	   • Security administrator: This is a role for the administration of security (policy and security contexts),
	
	   • Audit administrator: This is a role for administration of the audit policy and the evaluation of audit records,
	
	   • Staff: This is a user role for users allowed to use the newrole and su commands,
	
	   • User: This is a general user role without being allowed to use the newrole and su commands.
	
	 Users cannot interfere with these labels. The TOE uses SELinux with an appropriate SELinux policy to enforce the authoritative access control.

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. The TOE provides separation between different virtual machines and their resources as well as between virtual machines and the host system. The TOE as a host system operates the virtual machines like unprivileged applications.
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.
Protection mechanisms	The TOE provides mechanisms to prevent common buffer overflow and similar attacks. These mechanisms are used for the TSF and are available to untrusted code.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.5.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE:

Red Hat Enterprise Linux 6.2 with additional packages set up according to the Evaluated Configuration Guide [8]. This certificate covers a selected set of server systems based on x86 64bit processors from Intel and AMD. Other hardware might be covered in a seperate certificate.

For further details refer to 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 6.2 with KVM Virtualization for x86 Architectures

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Red Hat Enterprise Linux 6.2 Server (AMD64/Intel64T)	Release 6 Update 2	Download
2	SW	Evaluation package RPM EAL4_RHEL6.2 (e.g., cc-eal4-config-rhel62-0.33-1.noarch.rpm)	0.28.1	Download
3	DOC	EAL4 Evaluated Configuration Guide for Red Hat Enterprise Linux	V1.3	Download

No	Type	Identifier	Release	Form of Delivery
4	SW	Updates required: • Fix RHSA-2012:0124 • Fix RHBA-2012:0342 • Fix RHBA-2012:0338 • Fix RHEA-2012:0065 • Fix RHBA-2012:0134 • Fix RHBA-2012:0331 • Fix RHSA-2012:0050 • Fix RHBA-2012:0339 • Fix RHBA-2012:0337 • Fix RHBA-2012:0344 • Fix RHBA-2012:0360 • Fix RHBA-2012:0486	See package names	Download

Table 2: Deliverables of the TOE

The TOE is delivered from the developer, Red Hat, using the Red Hat delivery mechanism. There are several download components: the Red Hat Enterprise Linux Server 6.2 distribution and an additional package created specifically for the evaluation of RHEL 6.2 on the hardware platforms specified in the ST as well as specific update packages and the Evaluated Configuration Guide [8].

RHEL 6.2 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 to verify the checksums and the signatures.

The additional evaluation package contains the kickstart installation program and configuration files, as well as the Evaluated Configuration Guide. The package is securely provided by the developer, reviewed and built into an RPM by the Team Lead for the Security Technologies Team, signed by Release Engineering using the signing key referenced above before delivery, and electronically delivered by Red Hat's download site (RHN). Customers who download the package are advised to verify the signature.

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 (v. 6.2 for 64-bit x86_64)). The downloaded ISO image (no. 1 from table 2) is named according to release and architecture and has the following sha256 hash value:

rhel-server-6.2-x86_64-dvd.iso
3d2b25d4e7b919398c03fcc477188156277ea41763c8e4d08857c8841e773849

The user can verify the integrity of the ISO image by checking the hash value. Following the installation, the user can verify by looking at the content of /etc/release that the installed version is "Red Hat Enterprise Linux Server release 6.2".

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
- Cryptographically protected Remote Access
- Discrenationary Access
- Network Flow Control
- Sunbject Information Flow Control
- Identification and Authentication
- Management of I&A
- Trusted Channel to Remote IT
- Role Delegation
- Role Management
- Role Approval
- Remote Audit Trail
- Audit Analysis
- Labelled Security Information Flow
- Labelled Security Printing
- Maintenance of Security Labels
- Information Flow Control between Compartments
- Access Control to Resoures for Compartment
- Compartment unique Identification
- Data Separation for Compartments
- Management of Compartment Trust Anchor
- Runtime Protection

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, correct configration and setup of system, system maintenance, trusted physical environment, secure recovery mechanisms. Details can be found in the Security Target [6], chapter 4.2.

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.

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 kernel itself is structured into a number of subsystems which are explained in detail in the high-level design of the TOE. Those are:

- File and I/O Subsystem
  Implements all file system object related functions. Functions include those that allow a process to create, maintain, interact and delete file-system objects, such as regular files, directories, symbolic links, hard links, device special files, named pipes, and sockets.

- Process Subsystem
  Implements functions related to process and thread management. Functions include those that allow the creation, scheduling, execution, and deletion of process and thread subjects.

- Memory Subsystem
  Implements functions related to the management of a system's memory resources.

Functions include those that create and manage virtual memory, including management of page tables and paging algorithms.

- Networking Subsystem
  This subsystem implements UNIX and internet domain sockets as well as algorithms for scheduling network packets.

- IPC Subsystem
  Implements functions related to inter-process communication mechanisms. Functions include those that facilitate controlled sharing of information between processes, allowing them to share data and synchronize their execution in order to interact with a common resource.

- Audit Subsystem
  Implements the kernel functions required to intercept system calls and audit them in accordance with the auditing policy defined by the system administrator.

- Kernel Modules Subsystem
  This subsystem implements an infrastructure to support loadable modules. Functions include those that load and unload kernel modules.

- Device Driver Subsystem
  Implements support for various hardware devices through common, device independent interface.

- KVM
  The KVM subsystem provides the kernel parts of the virtualization.

- Kernel SELinux Subsystem
  This subsystem provides a framework for various access control policies. The TOE configuration utilizes this subsystem to implement MLS and separation of virtual machines.

- Cryptographic mechanisms
  Cryptographic mechanisms implemented in the kernel which can be used as a library for other kernel parts, if needed.

The trusted processes include the following subsystems:

- Identification and Authentication
  This subsystem includes all the processes that are require to identify and authenticate users. All those processes share a common set of functions (pluggable authentication modules (PAM)) that ensure that the same policy will be enforced with respect to identification and authentication of users. Successful as well as unsuccessful authentication attempts can be audited.

- Network Applications
  This subsystem includes the trusted processes implementing networking functions. The TOE supports SSH. The secure configuration as defined in the Security Target restricts the cipher suites that can be used for secure communication.

- System Management
  This subsystem includes the trusted commands a system administrator can use to manage users and groups, set the time and date and check the integrity of the installed packages.

- Batch Processing
  This subsystem includes the cron and at trusted processes that allow to execute user

programs at predefined time schedules. They ensure that the users are restricted to the same security policy restrictions that also apply when they start programs interactively.

● User Level Audit
This subsystem includes all the trusted processes and commands outside of the kernel required to collect, store and process audit records.

In addition to those functions 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:

● Identification and Authentication
The TOE provides identification and authentication using pluggable authentication modules (PAM) based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by the TOE. Other authentication methods (e. g. Kerberos authentication, token based authentication) that are supported by the TOE as pluggable authentication modules are not part of the evaluated configuration. Functions that ensure a basic password strength and limit the use of the su command and restrict root login to specific terminals are also included.

● Audit
The TOE provides the capability to audit a large number of events including individual system calls as well as events generated by trusted processes. Audit data is collected in regular files in ASCII format. The TOE provides a program for the purpose of searching the audit records.
The system administrator can define a rule base to restrict auditing to the events he is interested in. This includes the ability to restrict auditing to specific events, specific users, specific objects or a combination of all of this.
Audit records can be transferred to a remote audit daemon.

● Discretionary Access Control
Discretionary Access Control (DAC) restricts access to file system objects based on Access Control Lists (ACLs) that include the standard UNIX permissions for user, group and others. Access control mechanisms also protect IPC objects from unauthorized access.
The TOE includes the ext4 file system, which supports POSIX ACLs. This allows defining access rights to files within this type of file system down to the granularity of a single user.

● Mandatory Access Control
Mandatory Access Control (MAC) restricts access to objects based on labels assigned to subjects and objects. Sensitivity labels are automatically attached to processes and objects. The access control policy enforced using these labels is derived from the Bell-LaPadula access control model.
SELinux categories are attached to virtual machines and its resources. The access control policy enforced using these categories grant virtual machines access to resources if the category of the virtual machine is identical to the category of the accessed resource.
The TOE implements non-hierarchical categories to control access to virtual machines.

- Role-based access control
  Role-based access control (RBAC) allows separation of roles to eliminate the need for an all powerful system administrator.

- Object Reuse
  File system objects as well as memory and IPC objects will be cleared before they can be reused by a process belonging to a different user.

- Security Management
  The management of the security critical parameters of the TOE is performed by administrative users. A set of commands that require root privileges (or specific roles when RBAC is used) are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users that are not administrative users.

- Secure Communication
  The TOE supports the definition of trusted channels using SSH. Password based authentication is supported. Only a restricted number of cipher suites are supported for those protocols in the evaluated configuration. They are listed in the Security Target.

- Storage encryption
  The TOE supports encrypted block devices to provide storage confidentiality via dm_crypt.

- TSF Protection
  While in operation, the kernel software and data are protected by the hardware memory protection mechanisms. The memory and process management components of the kernel ensure a user process cannot access kernel storage or storage belonging to other processes.
  Non-kernel TSF software and data are protected by DAC and process isolation mechanisms. In the evaluated configuration, the reserved user ID root owns the directories and files that define the TSF configuration. In general, files and directories containing internal TSF data (e.g., configuration files, batch job queues) are also protected from reading by DAC permissions.
  The TOE and the hardware and firmware components are required to be physically protected from unauthorized access. The system kernel mediates all access to the hardware mechanisms themselves, other than program visible CPU instruction functions.
  In addition, mechanisms for protection against stack overflow attacks are provided.

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 [6].

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

7.1.1   Test Configuration

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

- IBM System p, Power 750
- IBM System x ,x3850 X5 E7520
- IBM System x, x3620 M3 E5620
- IBM System z, z10
- SGI, UV 1000
- HP ProLiant DL360 G6 (Xeon – base)
- HP ProLiant DL360 G7 (Xeon – mls)
- HP ProLiant DL385 G7 (Opteron
- Dell PowerEdge R72

The sponsor has performed his tests on the above listed hardware platforms. The software was installed and configured as defined in the Evaluated Configuration Guide [8] with additional software packages identified in the Test Plan. The test plan presents the arguments that those additional packages are within the boundary defined by the Security Target and do not constitute a violation of the evaluated configuration.

Please note that not all listed configurations are covered by this certificate. For details please refer to chapter 8 of this report.

7.1.2   Testing Approach

The test plan provided by the sponsor 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 TDS.

The sponsor 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. Most of the tests are automated tests.

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) apart from the dedicated 64bit syscalls in 32bit mode which is expected. The test systems were configured according to the ST [6] and the instructions in the [8].

7.1.3   Testing Results

The test results provided by the sponsor 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.

The developer did not test all machines of all families mentioned in the ST, but only one machine for each CPU 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

7.1.4   Test Coverage

The functional specification has identified the following different TSFI:

● system calls

● hypervisor calls

● security critical configuration files (TSF databases)

● trusted programs and the corresponding network protocol SSH v2.

The mapping provided by the sponsor 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 sponsor's test suite.

7.2   Evaluator Testing

7.2.1   Test Configuration

The evaluator has set up several systems, to cover more configurations as necessary for this certificate. The tests have been repeated on several of the configurations:

● IBM System p - Power 750

● IBM System x - x3850X5 E7520

● IBM System x - x3620M3 E5620

● IBM System z - z10

● SGI - UV 1000

● HP - ProLiant DL360 G7 (Intel Xeon)

● HP - ProLiant DL385 G7 (AMD Opteron)

● Dell - PowerEdge R720

Please note that not all listed configurations are covered by this certificate. For details please refer to chapter 8 of this report.

7.2.2   Independent Tests

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:

- The test cases examine some of the security functions of the TOE in more detail than the sponsor-supplied test cases. (Object reuse and DAC).

- The test cases cover aspects not included in the developer testing (verification of the ACL support in the archival tool, the use of /dev/random instead of /dev/urandom) and the use of address space randomization.

- As the sponsor-supplied test cases already cover the TOE in a broad sense the evaluator has devised only a small set of test cases.

The evaluator created several test cases for testing a few functional aspects where the sponsor test cases were not considered by the evaluator to be broad enough. During the evaluator's review of the test cases provided by the sponsor, the evaluator gained confidence in the sponsor testing effort and the depth of test coverage in the sponsor supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the evaluator devised only a small number of test cases.

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 sponsor'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 additional RPMs as well as the test cases and test tools were installed on the test machine by the developer according to the instructions in [8] and Test Plan, and verified by the evaluator. During the evaluation, the file system type ext4 was used for hard disk partitions on the test system. The configuration scripts triggered by the kickstart 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 [8]. The evaluator verified the configuration against the [8] before conducting the independent tests. The log files generated by the test cases were analyzed for completeness and failures.

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:

- Permission settings of relevant configuration files

- Verification of the use of SHA512 passwords

- Verification that SSH uses /dev/random instead of /dev/urandom

- Verification that SUID programs do not change the real UID

- Testing of object reuse in regular file system objects

- Check for data import / export with DAC enforcement

- Verification that the permission check during open() is enforced during read() and write()

- Verification of cleaning of environment for SUID/SGID binaries

- Verification of address space randomization

All tests passed successfully.

7.2.3   Evaluator Penetration Testing

The evaluator took the following approach to derive penetration tests for the TOE: First the evaluator checked common sources for vulnerabilities of the Linux operating system in general and the TOE in particular to determine:

- whether the reported vulnerability would affect the evaluated configuration of the TOE in its intended environment. If yes, the evaluator performed a vulnerability analysis.

- if the reported vulnerability has already been fixed in the evaluated configuration of the TOE.

Beside those vulnerabilities reported in common sources the evaluator checked the other evaluation reports for potential vulnerabilities mentioned there. None were identified.

The evaluator decided to not generate simple penetration tests, but instead to perform a source code analysis far deeper than usually done for this evaluation level for some of the identified potential vulnerabilities. The following reasons apply:

- The TOE as an Open Source product is checked for obvious vulnerabilities quite extensively by the Open Source community making the development of high level, simple penetration tests ineffective.

- The TOE as an Open Source product is delivered with the full source code, thus allowing the evaluator to perform an analysis to a depth usually not possible for products evaluated at this level. In general, the evaluator believes that a vulnerability analysis based on source code audit is far more accurate than a test case. Per nature, a perceived vulnerability is usually obscure in nature and therefore only exploitable when meeting certain constraints. As the testing may not meet all constraints, a test case indicating that there is no vulnerability does not demonstrate that no vulnerability is present.

- As the source code is publicly available, the evaluator has to assume that potential attackers use the source code to search for potential attack vectors.

The evaluator has performed his analysis on the TOE source code that was installed from the developer distributed source code DVD.

The penetration testing addressed the following security functions:

- TSF Protection

- VM separation

No residual vulnerabilities for the TOE that are exploitable with the assumed attack potential stated in the ST were identified.

8   Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration is documented in the Evaluated Configuration Guide ([8]). It is based on Red Hat Enterprise Linux 6.2 (RHEL 6.2) with additional packages as listed in table 2. The software is to be used on the following hardware platforms specified in the Security Target [6]:

- IBM based on x86 64bit Intel Xeon processors:

- IBM System x: x3400 M2, x3400 M3, x3500 M2, x3500 M3, x3550 M2, x3550 M3, x3620 M3, x3630 M3, x3650 M2, x3650 M3
- IBM BladeCenter: HS22 and HS22V
- IBM iDataPlex: dx360 M2, dx360 M3
- IBM X5 systems: x3850 X5, x3950 X5, x3690 X5

● HP based on x86 64bit Intel Xeon processors:
- HP Proliant ML 100 and 300 series G6 product line
- HP Proliant DL 100 series G6, 300 series G6 and G7, 500 series G7, 900 series G7 product line
- HP ProLiant BL 200 series G6 and G7, 400 series G6 and G7, 600 series G5, 600 series G7 product line
- HP ProLiant SL 100 series G6 product line

● HP based on AMD64 processors:
- HP Proliant DL 100 series G7, 500 series G7, 700 series G6 product line
- HP Proliant DL 385 G7
- HP ProLiant BL 600 series G6 product line
- HP ProLiant SL 100 series G7 product line

● SGI UV
- SGI UV 1000

● Dell based on x86 64bit Intel:
- Dell PowerEdge R720, R620, R820, R520, R320, R420
- Dell PowerEdge T620, T420, T320
- Dell PowerEdge M620, M520, M420, M820

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) [9] 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.

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 – Labeled Security, Version 2.0, 28 May 2010,
    OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010 [7]

● 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

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 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). This holds for:
–   the TOE Security functionality according to the following table and
–   for other usage of encryption and decryption within the TOE.

Algorithm	Key Length	Inteded Purpose	Security Function	Implementation Standard
AES	128 bits, 192 bits, 256 bits	Encryption / Decryption	Protected Data Transfer, Protection for Data at Rest	RFC 4253
TDES	168 bits	Encryption / Decryption	Protected Data Transfer	RFC 4253
RSA	1024 bits, 2048 bits, 3072 bits	Authentication, Key Exchange	Identification and Authentication, Protected Data Transfer	U.S. NIST FIPS PUB 186-3
DSA	L=1024, N=160 bits	Authentication, Key Exchange	Identification and Authentication, Protected Data Transfer	U.S. NIST FIPS PUB 186-3
Serpent	128, 196 or 256 bit	Encryption / Decryption	Protection of Data at Rest	http://www.cl.cam.ac.uk/~rja14/Papers/serpent.pdf
Twofish	128, 196 or 256 bit	Encryption / Decryption	Protection of Data at Rest	http://www.schneier.com/paper-twofish-paper.html
SHA-1	-	Message Digest	Protection of Data at Rest, Protected Data Transfer	FIPS 180-3
SHA-2 (224 bit) SHA-2	-	Message Digest	Protection for Data at Rest, Identification and Authentication	FIPS 180-3

Algorithm	Key Length	Inteded Purpose	Security Function	Implementation Standard
(256 bit) SHA-2 (384 bit) SHA-2 (512 bit)				

Table 3: Supported Algorithms

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 for 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

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

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.

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

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

Informal - Expressed in natural language.

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

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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 3, July 2009
       Part 2: Security functional components, Revision 3, July 2009
       Part 3: Security assurance components, Revision 3, July 2009

[2]   Common Methodology for Information Technology Security Evaluation (CEM),
       Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3]   BSI certification: Procedural Description (BSI 7125)

[4]   Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5]   German IT Security Certificates (BSI 7148), periodically updated list published also
       in the BSI Website

[6]   Security Target BSI-DSZ-CC-0754-2012, Version 1.8, October 8th 2012, Red Hat
       Enterprise Linux, Version 6.2 with KVM Virtualization for x86 Architectures Security
       Target, Red Hat, Inc.

[7]   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 – Labeled Security, Version 2.0, 28 May 2010,
       OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010

[8]   Guidance Documentation for the TOE, Version 1.3, July 6th 2012, EAL4 Evaluated
       Configuration Guide for Red Hat Enterprise Linux

[9]   Evaluation Technical Report, Version 4, October 9th 2012, Final Evaluation
       Technical Report, atsec information security GmbH (confidential document)

[10]   Configuration lists for the TOE: CI list of CC evidence, test cases, test plans, man
       pages, scripts and tools (Mai 4th 2012), Kickstart RPM CI list (Mai 25th 2012),
       Kickstart RPM CI list from Git (July 23rd 2012), CI list from CVS showing yaboot
       bootmanager for pSeries platform (August 9th 2012), CI list from CVS showing zipl
       bootmanager for zSeries platform (August 9th 2012), (all confidential documents)

---

[8]specifically

- AIS 20, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

- AIS 38, Version 2.9, Reuse of evaluation results

C   Excerpts from the Criteria

CC Part1:

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

Assurance Class	Assurance Components
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 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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"

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

"Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested (chapter 8.4)

"Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked (chapter 8.5)

"Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

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."

This page is intentionally left blank

D   Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.