Federal Office
for Information Security

# Certification Report

# BSI-DSZ-CC-0711-2012

for

# IBM AIX 7 for POWER, V7.1 Technology level 7100-00-03 with optional IBM Virtual I/O Server V2.2

from

# IBM Corporation

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-0711-2012

**IBM AIX 7 for POWER,** V7.1 Technology level 7100-00-03 with optional IBM Virtual I/O Server V2.2

| | |
|---|---|
| from | IBM Corporation |
| PP Conformance: | Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010<br>OSPP Extended Packages:<br>(1) General Purpose Cryptography, (2) Integrity Verification, (3) Virtualization, (4) Advanced Management, (5) Labeled Security all Version 2.0, 28 May 2010 |
| Functionality: | PP conformant<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>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, 20 August 2012

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski
Head of Department

L.S.

**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

This page is intentionally left blank.

# 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 IBM AIX 7 for POWER, V7.1 Technology level 7100-00-03 with optional IBM Virtual I/O Server V2.2 has undergone the certification procedure at BSI.

The evaluation of the product IBM AIX 7 for POWER, V7.1 Technology level 7100-00-03 with optional IBM Virtual I/O Server V2.2 was conducted by atsec information security GmbH. The evaluation was completed on 8 August 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: IBM Corporation.

The product was developed by: IBM Corporation.

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 IBM AIX 7 for POWER, V7.1 Technology level 7100-00-03 with optional IBM Virtual I/O Server V2.2 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] IBM Corporation
11501 Burnet RD
Austin,TX 78758-3400
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 target of evaluation (TOE) is the AIX Version 7.1 operating system and the optional IBM Virtual I/O Server (VIOS) Version 2.2 including ifixes shipped as part of PRPQ P91209.

AIX is a general purpose, multi-user, multi-tasking operating system. It is compliant with all major international standards for UNIX systems. It provides a platform for a variety of applications in the governmental and commercial environment. AIX is available on a broad range of computer systems from IBM, ranging from departmental servers to multi-processor enterprise servers, and is capable of running in an LPAR (Logical Partitioning) environment.

Several servers running AIX 7.1 (any combination of BAS mode systems and LAS mode system scan be used) can be connected to form a distributed system, but not all components of such a system are components of the TOE. The communication aspects within AIX 7.1 used for this connection are also part of the evaluation. It is assumed that the communication links themselves are protected against interception and manipulation by measures which are outside the scope of this evaluation.

In LAS mode, the TOE enforces MAC, MIC, DAC, and TCB control policies to implement security goals, such as confidentiality, integrity, and accountability. LAS mode can operate in a network or stand-alone configuration. In a network configuration, LAS mode supports BSO/ESO/CIPSO/RIPSO and provides network filtering on incoming and outgoing packets, based on network interface and host filtering rules.

The AIX evaluation shall consist of a closed network of high-end, mid-range and low-end IBM System p POWER6 and POWER7 servers running the TOE. In addition, each server may optionally run VIOS.

The TOE Security Functionality (TSF) consists of those parts of AIX that run in kernel mode plus some trusted processes. These are the functions that enforce the security policy as defined in the Security Target. Tools and commands executed in user mode that are used by the system administrator 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.

Table and Table 2 provide a guide for what is supported in BAS mode and what is supported in LAS mode. An ‘X' means that the mode supports the description.

| BAS Mode | LAS Mode | TOE Description |
|---|---|---|
| x | x | The TOE includes installation from CD-ROM. |
| x | x | The TOE includes the Virtual Input/Output Server (VIOS) which allows for the virtualization of SCSI drives and network adapters. |
| x | x | System administration tools include the smitty non-graphical system management tool. The WebSM administrative tool is excluded. |
| x | | The TOE includes standard networking applications, such as ftp, rlogin, rsh, and NFS. Port filtering will be used to protect network applications which might otherwise have security exposures. |
| | x | The TOE includes the following networking applications: telnet and ftp. It also includes NFS as a single level file system. |
| x | | The TOE includes the X-Window graphical interface and many X-Window applications. |
| | x | The TOE supports BSO/ESO/CIPSO/RIPSO for IPv4 with an AIX specific implementation for IPv6 and provides network filtering on incoming and outgoing packets, based on network interface and host filtering rules. |

**Table 1: BAS mode vs. LAS mode for TOE**

| BAS Mode | LAS Mode | Operational Environment Description |
|---|---|---|
| x | x | The Operational Environment includes the hardware and the BootProm firmware. |
| x | x | The Operational Environment includes applications that are not evaluated, but are used as unprivileged tools to access public system services, for example the Mozilla web browser or the Adobe Acrobat Reader to access the supplied online documentation(which is provided in HTML and PDF formats). No HTTP server is included in the evaluated configuration. |
| x | x | The Operational Environment includes LDAP for maintaining TOE authentication data. |
| x | x | The Operational Environment includes Kerberos for aiding in establishing a trusted channel between NFSv4 clients and servers. |

**Table 2: BAS mode vs. LAS mode for Operational Environment**

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,
OSPP Extended Package – General Purpose Cryptography, Version 2.0, 28 May 2010, OSPP Extended Package – Integrity Verification , Version 2.0, 28 May 2010, OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010, OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010, OSPP Extended Package – Labeled Security, 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 6.1. 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:

- AIX:
  - Identification and authentication
  - Auditing
  - Discretionary access control
  - Object reuse
  - Security management
  - TSF protection
  - Privileges, authorizations, roles, and superuser emulation
  - TCB protection
  - Trusted Execution (TE)
  - Networking
  - Workload Partitions (WPARs)
  - Cryptographic Framework
  - Mandatory access control (LAS mode only)
  - Mandatory integrity control (LAS mode only)
  - Trusted Network (LAS mode only)
- VIOS:
  - Identification & authentication
  - Discretionary access control
  - Role-based access control
  - Security management

For more details please refer to the Security Target [6], chapter 1.5.1.

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.

The evaluated configuration is documented in the AIX Release Notes [9]. This document 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.

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:

**IBM AIX 7 for POWER,** V7.1 Technology level 7100-00-03
with optional IBM Virtual I/O Server V2.2

The following table outlines the TOE deliverables:

| No | Type | Identifier | Form of Delivery |
|---|---|---|---|
| 1. | SW | • AIX Base Operating System(bos LPP)<br>• AIX supported devices (devices LPP)<br>• AIX printer drivers and control files (printers LPP)<br>• System management tools (sysmgt LPP)<br>• X Windows server,libraries, and applications (X11 LPP)<br>• Kerberos client (optional) (krb5.client LPP)<br>• TDS (LDAP) client (optional) (ldap.client LPP)<br>• CliC cryptographic module (clic LPP)<br>• PRPQP91209 | Physical delivery by ordering the PRPQ |
| 2. | DOC | Technical Reference: Communications, Volume 1<br>Version: SC23-6738-00<br>Date received: Oct 2010<br>SHA-256: 771b14348c6410c495b7c4d6fc934ec781d941f64f9b85271b037dd5e48d31c7<br><br>Technical Reference: Communications, Volume 2<br>Version: SC23-6739-00<br>Date received: Oct 2010<br>SHA-256:325395bce1b1c279838c63f1b2513ace5adc14e9b93f27d30de83c6e291fac40 | Electronic delivery via IBM Infocenter |

| No | Type | Identifier | Form of Delivery |
|---|---|---|---|
| 3. | DOC | Commands Reference, Volume 1<br>Version: SC23-6709-00<br>Date received: Sep 2010<br>SHA-256: 8a982de2980453971b6227d123ae83189f632c22f6b22b715ca03277fb975da5<br><br>Commands Reference, Volume 2<br>Version: SC23-6710-00<br>Date received: Sep 2010<br>SHA-256: 71bc345d78d4beb8c948ed21b40e54e6406f0071bf26d86533c675bbc8367634<br><br>Commands Reference, Volume 3<br>Version: SC23-6711-00<br>Date received: Sep 2010<br>SHA-256: 7ff2c6fd019633e67b410ffbf5c122c09b274a356e1fa922d53f7cfdaddb48b5<br><br>Commands Reference, Volume 4<br>Version: SC23-6712-00<br>Date received: Sep 2010<br>SHA-256: aba07585de26ad3f8cd59021fd3c5814509702a22e53ebafbeea0465ea696e4b<br><br>Commands Reference, Volume 5<br>Version: SC23-6713-00<br>Date received: Sep 2010<br>SHA-256: 4b1dfbd55b5406ad7735aa47612a5e6fdbcde16eb308a2a71431905e54e8705b<br><br>Commands Reference, Volume 6<br>Version: SC23-6714-00<br>Date received: Sep 2010<br>SHA-256: b17ed1b42b71bb9775e1e12e1dc13c9e97c0104272bcaa33be0a04b442ccc8c3 | Electronic delivery via IBM Infocenter |
| 4. | DOC | Understanding the Diagnostic Subsystem for AIX<br>Version: SC23-6742-00<br>Date: Sep 2010<br>SHA-256: c6f739944744159db494d9d98439f296f25c9fb8a12987f33d55933daff8346d | Electronic delivery via IBM Infocenter |
| 5. | DOC | Files Reference<br>Version: SC23-6717-00<br>Date: Oct 2010<br>SHA-256: 3067f66fa711a2c53dfc08e2372d7eb477c7451dfe9c3b6cc519991db81e2404 | Electronic delivery via IBM Infocenter |
| 6. | DOC | General Programming Concepts: Writing and Debugging Programs<br>Version: SC23-6718-00<br>Date: Oct 2010<br>SHA-256: d43bb6f1e7c140ca88ed555a0c0980a3b052aa9de357b178413501514347222a | Electronic delivery via IBM Infocenter |
| 7. | DOC | Kernel Extensions and Device Support Programming Concepts<br>Version: First Edition<br>Date: Sep 2010<br>SHA-256: f2b16c9ebc2af445e26146fdda3492f62cd7291a5dfd8fee235a2256b76fda92 | Electronic delivery via IBM Infocenter |
| 8. | DOC | AIX 7.1 Technical Reference: Kernel and Subsystems, Volume 1<br>Version: First Edition<br>Date: Sep 2010<br>SHA-256: c5bc06c21041710aaa3c510427205a31ccd15b6aa39b3a61af1e3d8e97d309a8<br><br>AIX 7.1 Technical Reference: Kernel and Subsystems, Volume 2<br>Version: First Edition<br>Date: Sep 2010<br>SHA-256: 73ea0f7f2f8b7396245a66b6e49a1f54a26bdcdc0da8abce88504ee0a36ef9db | Electronic delivery via IBM Infocenter |
| 9. | DOC | Operating system and device management<br>Version: SC23-6730-00<br>Date: Oct 2010<br>SHA-256: 885b735ea0b864300f27003542ba126b285659ef526e3e36cd4078e0beb7ab18 | Electronic delivery via IBM Infocenter |
| 10. | DOC | AIX Version 7.1 Release Notes<br>Version: GI11-9815-01<br>Date: 2012-08-06<br>SHA-256: 780e5c5135c05c0e9847b42fac2696a567948f4ebd550f5476c62040347dc314 | Electronic delivery via IBM Infocenter |
| 11. | DOC | AIX Version 7.1: Security<br>Version: SC23-6735-00<br>Date: Sep 2011<br>SHA-256: 38208a80c229489990331bc4279705c9ee5fff85887f94ecda1fee14664a12a3 | Electronic delivery via IBM Infocenter |

| No | Type | Identifier | Form of Delivery |
|---|---|---|---|
| 12. | DOC | Networks and Communications Management<br>Version: SC23-6729-00<br>Date: Oct 2010<br>SHA-256: 14e81d36fc5cb2b7370a0a0d92e0bc43a1611a9936d9ea64dd03026a0d6b6e84 | Electronic delivery via IBM Infocenter |
| 13. | DOC | AIX 7.1 Technical Reference: Base Operating System and Extensions, Volume 1<br>Version: SC23-6736-00<br>Date: Oct 2010<br>SHA-256: 80cd69a578494cd8199977c8c0e29dbae8b7670060a659818ceadd4b2044ac81<br><br>AIX 7.1 Technical Reference: Base Operating System and Extensions,Volume 2<br>Version: SC23-6737-00<br>Date: Oct 2010<br>SHA-256: 29b5a93791f817cc69eff1b35aaaf860812ba9e95070b0744f597b052b5534f4 | Electronic delivery via IBM Infocenter |
| 14. | DOC | Virtual I/O Server and Integrated Virtualization Manager commands<br>Version: 2.1.2.0<br>Date: 2009<br>SHA-256: cef8c826da9f6d696b830ba7f9286e26e31c15c4682251704630f2ec90257f1d | Electronic delivery via IBM Infocenter |
| 15. | DOC | Virtual I/O Server<br>Version: 2.2.0.12<br>Date: 2011<br>SHA-256: 8277c21d56b098105db4156e3b31db94e90326a583831194112d4dd084e0b5cb | Electronic delivery via IBM Infocenter |
| 16. | DOC | IBM Workload Partitions for AIX<br>Date: Oct 2010<br>SHA-256: 245bc3a7ffa4339ed69bccc0539ce5ec3fb39555b357fb691cb8dca72ecc6cc9 | Electronic delivery via IBM Infocenter |

**Table 3: Deliverables of the TOE**

The integrity of the TOE parts delivered via the IBM Infocenter should be checked by recomputing the SHA-256 checksums and comparing those with the ones above.

# 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:

- The TSF must be able to record defined security-relevant events.
- The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication.
- The TSF must control access of subjects and/or users to named resources based on identity of the object.
- The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE and the TOE itself in accordance with its security policy.
- The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.
- The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.
- The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.

- The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.
- The TOE must allow roles assigned to users for performing security-relevant management tasks to be delegated to other users in accordance with the security policy.
- The TOE must allow security management actions based on roles to be assigned to different users.
- The TOE must prevent the execution of user actions allowed by a specific permission until a second user with a different permission approves this action.
- The TSF must provide the following cryptographic services for general use by authorized entities: symmetric and asymmetric ciphers, message digest generation, symmetric and asymmetric key generation.
- The TOE shall be able to verify the integrity of both TSF code and TSF data to ensure that they have not been modified when compared to the integrity information in the integrity database.
- The TOE shall be able to verify the integrity of user data to ensure that it has not been modified when compared to the integrity information in the integrity database.
- The TOE shall perform pre-defined actions upon detection of a breach of integrity.
- The TOE shall be able to allow authorized users to update the integrity verification database covering TSF data, the TSF code, and user data.
- The TOE will control information flow between entities and resources based on the sensitivity labels of users and resources (LAS mode only).
- The TOE will provide the capability to mark printed output with accurate labels based on the sensitivity label of the subject requesting the output (LAS mode only).
- The TOE will provide the capability to label all subjects, and all objects accessible by subjects, to restrict information flow based on the sensitivity labels (LAS mode only).
- The TOE will control information flow between compartments under the control of the TOE, based on security attributes of these compartments and potentially other TSF data (e.g.,security attributes of objects).
- The TOE will control access of compartments to objects and resources under its control based on: security attributes of the objects, security attributes of the compartment that attempts to access the object, and the type of access attempted.
- For each access request, the TOE is able to identify the compartment requesting to access resources, objects or information.
- The TOE shall offer administrators a mechanism to overwrite user-accessible blocks of SCSI hard disk drives with predefined bit patterns.
- The TOE shall control access to resources based on the integrity level of the information being accessed and the integrity level of the subject attempting to access that information (LAS mode only).

- The TOE shall prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations.
- The TOE shall ensure that only authorized users gain access to protected TOE resources and that this access is controlled by authorized administrators.
- The TOE shall detect inconsistencies, corruption, and inaccessibility in the RBAC-related databases and enforce a fail secure policy.
- The TOE shall allow hierarchical definitions of roles. Hierarchical definition of roles means the ability to define roles in terms of other roles.
- The TOE shall provide the capability of enforcing 'separation of duties', so that no single user has to be granted the right to perform all operations on important information.
- The TOE shall offer a mechanism to prevent the execution of code on the stack of selected processes.
- The TOE shall control write and/or execute access to resources protected as part of the trusted computing base as specified by an authorized administrator.
- The TOE shall control access between the TOE and other systems based on host security attributes and the network interface on which packets are sent or received (LAS mode only).
- The TSF shall ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only (VIOS only).
- The TSF shall provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and shall ensure that only authorized users are able to access such functionality (VIOS only).
- The TSF shall control access between VIOS Ethernet adapter device drivers and VIOS Ethernet device drivers acting on behalf of groups of LPAR partitions sharing a virtual network (VIOS only).
- The TOE shall prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations (VIOS only).
- The TOE shall allow hierarchical definitions of roles. Hierarchical definition of roles means the ability to define roles in terms of other roles (VIOS only).
- The TOE shall provide the capability of enforcing 'separation of duties', so that no single user has to be granted the right to perform all operations on important information (VIOS only).
- The TSF shall control access between LPAR partitions and logical/physical volumes and VIOS SCSI device drivers acting on behalf of a group of LPAR partitions (VIOS only).

# 4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target [6] 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 individuals, capable of managing the TOE and the security of the information it contains.
- 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 from any attack that may cause those functions to provide false results.
- Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner.
- Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed,installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
- 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 those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives.
- 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.
- The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy
- The operational environment shall perform checks that ensure the integrity of the TSF code and TSF data loaded and executed before the successful execution of the integrity verification TSF.
- The operational environment shall ensure that the TSF code and TSF data (when in operation)cannot be manipulated or intercepted by entities not under the control of the TOE.
- The underlying hardware must protect the resources assigned to the TOE's logical partition against access from software running in a different logical partition.
- Those responsible for the TOE are competent and trustworthy individuals,capable of managing the TOE and the security of the information it contains (VIOS only).
- VIOS only: Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner (VIOS only).
- Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE (VIOS only).

- Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period (VIOS only).
- Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives (VIOS only).
- 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 (VIOS only).

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

# 5 Architectural Information

## 5.1 Major structural units of the TOE

The TOE contains the following structural units:

- The kernel, which executes in system mode.
- A set of trusted processes that execute in user mode but with root privileges. They also provide some of the security functions of the TOE.
- A set of configuration files that define the system configuration. Those files are named the “TSF database” and need to be protected by the access control mechanisms of the TOE such that they can only be modified by the system administrator.
- VIOS providing access to shared SCSI and Ethernet resources.

## 5.2 Security functions

The following sections present a summary of the security features that the TOE offers. These security features are supported by domain separation and reference mediation, which ensure that the features are always invoked and cannot be bypassed.

### 5.2.1 AIX

#### *5.2.1.1 Identification and authentication*

AIX provides identification and authentication (I&A) based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by AIX. The evaluated configurations for I&A are:

- The file-based authentication method (the default configuration for authentication), which uses passwords to authenticate users.
- The LDAP authentication method configured for UNIX-type authentication, which uses passwords to authenticate users. (In the UNIX-type configuration, LDAP only stores the data used for I&A. It does not perform I&A for AIX. AIX must communicate with the LDAP server across an SSLv3 / TLSv1 connection.)
- The NAS (Kerberos Version 5) authentication method, but limited to NFSv4 client-server authentication for establishing trusted channel communications between the NFSv4 client and server.

Other authentication methods (e. g. Kerberos authentication as a general AIX authentication) that are supported by AIX in general are not part of the evaluated configuration. Especially pluggable authentication modules that, for example would allow the use a token based authentication process, are not part of the evaluated configuration.

All individual users are assigned a unique user identifier. This user identifier supports individual accountability. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions.

IBM Tivoli Directory Server (TDS) 6.1 and 6.2 are used for the LDAP service. The TDS client interface used by AIX uses the IBM Global Services Kit (GSKit) for performing the SSL services. The client interface, including GSKit, is part of the TOE. The client interface, including GSKit, is part of the Operational Environment.

#### *5.2.1.2 Auditing*

AIX can collect extensive auditing information about security related actions taken or attempted by users, ensuring that users are accountable for their actions.

For each event record, the audit event logger prefixes an audit header to the event-specific information. This header identifies the user and process for which this event is being audited, as well as the time of the event. The code that detects the event supplies the event type and return code or status and optionally, additional event-specific information (the event tail). Event-specific information consists of object names (for example, files refused access or tty used in failed login attempts), subroutine parameters, and other modified information.

This audit trail can be analyzed to identify attempts to compromise security and determine the extent of the compromise. The audit tools can also extract audit records of events involving objects and/or subjects having specified security attributes.

#### *5.2.1.3 Discretionary access control*

Discretionary Access Control (DAC) restricts access to objects, such as files and is based on Access Control Lists (ACLs) and the standard UNIX permissions for user, group and others. Access control mechanisms also protect IPC objects from unauthorized access. BAS mode supports ACLs on sockets for TCP connections. LAS mode supports ACLs on network ports and interfaces.

In addition, AIX supports the Encrypted File System (EFS) which allows for the encryption and decryption of files using the Advanced Encryption Standard (AES). File encryption works as a type of access control mechanism. The user must have DAC access and have access to the file's encryption key in order to decrypt the file's content. AIX uses the IBM CryptoLite for C (CliC) cryptographic module for EFS encryption and decryption.

#### *5.2.1.4 Object reuse*

All resources are protected from Object Reuse (scavenging) by one of three techniques: explicit initialization, explicit clearing, or storage management. Four general techniques are used to meet this requirement:

- Explicit Initialization: The resource's contents are explicitly and completely initialized to a known state before the resource is made accessible to a subject after creation.
- Explicit Clearing: The resource's contents are explicitly cleared to a known state when the resource is returned for re-use.

- Storage Management: The storage making up the resource is managed to ensure that uninitialized storage is never accessible.
- Erase Disk: AIX offers as part of its diagnostic subsystem an Erase Disc service aid that can be invoked by the administrator to overwrite all data currently stored in user-accessible blocks of a disk with predefined bit patterns. This mechanism ensures that data is made inaccessible to all users, including administrators as long as the hard disk remains within the system. This mechanism is not intended to defend against a sophisticated forensic analysis by disassembling the hard disk.

#### *5.2.1.5 Security management*

The management of the security critical parameters of AIX is performed by administrative users. A set of commands that require system administrator privileges 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.

In BAS mode and LAS mode, security management can be split between different roles.

#### *5.2.1.6 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.

TSF software and data, files and directories, kernel objects, IPC and networks sockets/packets are protected by TCB, DAC, and process isolation mechanisms. LAS mode provides additional mechanisms of MAC and MIC.

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.

The system administrator has the ability to start a program that checks the hardware for correct operation.

LAS Mode Only: The operational mode of AIX is intended to be the standard operating mode of the machine. The restrictions associated with operational mode cannot be overridden or bypassed by any mechanism. These restrictions are:

- the system security flags (SSFs) cannot be modified
- objects with the file security flags (FSFs) FSF_TLIB and FSF_TLIB_PROC set cannot be created, modified, or deleted

#### *5.2.1.7 Privileges, authorizations, roles, and superuser emulation*

The TOE implements a privilege mechanism within the kernel that allows users to implement the least privilege principle. A privilege is an attribute of a process that allows the process to bypass specific restrictions and limitations of the system. Privileges are associated only with processes, not user accounts. Privileges are used to override security constraints, to permit expanded use of certain system resources such as memory and disk space, and to adjust the performance and priority of the process. Restricting privileges on a process limits the damage that can result if an operation is improperly performed. Untrusted programs must not have any privileges assigned to them. The ST [6] describes

both a “root enabled mode” and a “root disabled mode” available in BAS mode,but only “root enabled mode” is allowed in the evaluated configuration of BAS mode. All mention of root enabled mode and root disabled mode refer to a BAS mode system only. (In root enabled mode, the ‘root' user has the typical ‘root' authority found in previous versions of AIX. In root disabled mode, the ‘root' user has its authority reduced to the equivalence of an ordinary user.) Only root disabled mode is supported/allowed in LAS mode.

The TOE least privilege mechanism can take the place of the traditional user ID 0 (superuser/root) mechanism of UNIX. In LAS mode, user ID 0 is treated exactly like any other system user ID unless superuser emulation is in effect for the process. In BAS mode with root enabled mode enabled, user ID 0 supports the traditional superuser mechanism.

Privileges can be associated with executable files and assigned to an executing process, similar to the way the setuid bit on a file modifies the executing process's user ID. A process can also be prevented from acquiring privileges via the exec mechanism. Privileges can be used directly within a user-level program that is responsible for mediating or enforcing security by having the program retrieve its privilege set from the kernel and to make decisions based on the presence or absence of specific privileges. A process can temporarily disable one or more of its privileges if the process needs to perform an action on the system without bypassing the system security policy.

The TOE supports the policy of separation of duties, which provides reducing the potential damage from a corrupt user or administrator, and places limits on the authority of the user or administrator for the compartmentalization of responsibility. Authorizations provide a mechanism to grant rights to users to perform particular actions and run particular programs, such as programs that will run with privileges to bypass MAC, MIC, or DAC limitations. Each authorization has a well-defined set of functions that can be performed by users who are granted that authorization. There are two types of authorized users: administrative role users and ordinary users. An administrative user is any authorized user that has one or more of the RBAC related authorizations (see the next paragraph for a discussion on RBAC). An ordinary user has no RBAC authorizations.

A role-based access control (RBAC) mechanism is implemented in AIX. Roles are predefined collections of authorizations that can be assigned to users. AIX comes with a set of predefined roles. It also allows system administrators to create new roles for their environment. AIX has two types of RBAC: Legacy RBAC and Enhanced RBAC. The evaluated configuration uses Enhanced RBAC only. All references to RBAC in this document imply Enhanced RBAC unless other wise specified.

In addition to RBAC functions, combined roles or role based approval can be implemented according to the users needs via the "n-man rule" functionality based on the authexec command which will execute other commands only after all required roles have authenticated. Commands needing the n-man rule are listed in the privcmds database and cannot be executed outside of the control of the authexec command.

A program has the ability to query the active authorizations associated with the user running the program, and the program can behave differently and use different privileges based on the authorization set of the user running the program. For the evaluated configuration, administrators (or administrative users) are defined as all users that have any authorization assigned to them. All user IDs below 205 are considered system IDs; they are typically used for daemons and other trusted applications.

Additionally, AIX provides a Privileged Commands (privcmds) database for granting privileges and setuid/setgid capabilities to trusted executables at runtime when a user has

the proper authorizations. When the kernel invokes a program, it checks the database for the existence of the program. If the program exists and the user has the proper authorizations, the discretionary access control on the program is ignored and the program is invoked with the privileges and/or setuid/setgid specified in the privcmds database.

The TOE provides a superuser emulation mechanism that allows the system to operate similar to a standard UNIX system. Superuser emulation can be enabled for specific processes while leaving all other processes running under the standard TOE least privilege and authorization mechanisms. There are several ways in which a process can emulate superuser:

1. A process can be granted all privileges on the system, regardless of its user ID.
2. Using the PV_SU_ROOT privilege, a process can be granted all privileges associated with standard AIX/UNIX superuser regardless of its user ID, such as the privileges to bypass any DAC restrictions and to management the auditing mechanism, but not privileges that are specific to the TOE-provided augmentation of standard AIX/UNIX security functionality, such as the privileges to modify kernel authorization tables, override MAC checks, etc.
3. Alternatively, the PV_SU_EMUL privilege can be set to grant processes all privileges associated with standard AIX/UNIX superuser when their process user ID is 0.
4. A process can be granted all authorizations/roles regardless of its user ID.
5. A process can be granted a “virtual user ID” of 0 so that queries to the kernel for its user ID will return 0 even regardless of the actual user ID associated with the process.

#### *5.2.1.8 TCB protection*

The TOE provides the concept of a Trusted Computing Base (TCB). Kernel, device drivers, system administration utilities, and other critical software that is used to enforce and administer the security of the system are part of this TCB. In addition, any file system object in the TOE (file, directory, device, etc.) can be marked with a TCB flag: FSF_TLIB. Alternatively, executables can be marked with the FSF_TLIB_PROC flag. The TCB is subject to several bypass control mechanisms enforced by the TOE, such as additional access control and integrity protection. Changes to objects being flagged as TCB objects can only be made when the system is in configuration mode or when the system security flag (SSF) *trustedlib_enabled* is disabled.

The integrity of objects in the TCB database is verified at every system startup and at the request of an authorized administrator.

#### *5.2.1.9 Trusted Execution (TE)*

In addition to the TCB, the TOE also supports a more modern form of integrity protection by monitoring files for integrity violations at access. The Trusted Execution function allows the administrator to define system and user resources for which changes to the resource are checked at access time resulting in denied access when the resource has been modified therefore preventing the execution of trojaned programs or libraries as well as the use of configuration files that have been tampered with. The checking is based on verifying SHA-256 checksums. The interface for managing the trusted execution function is the *trustchk* command.

#### *5.2.1.10 Networking*

*Protected remote access:*

The TOE supports IPsec for protected remote access connections. IPsec provides integrity and confidentiality of the transported data and is able to authenticate the end points.

*IP filtering:*

The TOE supports IP filtering of packets flowing to and through the TOE. IP packet flow can be permitted or denied based on several criteria/rules including presumed source address, destination address, and destination ports. IP packet filtering includes time-based rules where packet flow can be permitted or denied for a limited period of time after which the rules change.

#### *5.2.1.11 Workload Partitions (WPARs)*

AIX supports virtual environments called Workload Partitions (WPARs) which provide virtual AIX environments within AIX. WPARs provide process isolation so that applications can be installed and tested in a virtual environment. AIX supports two types of WPARs: System WPARs and Application WPARs.

A System WPAR is a virtual AIX system with its own set of users, administrators, hostname, network addresses, process isolation, IPC isolation, and file system isolation. An Application WPAR is similar to a System WPAR except without file system isolation. With the advent of WPARs, the main AIX environment is now called the Global environment. Multiple WPARs can be created and executed within the Global environment by a system administrator.

#### *5.2.1.12 Cryptographic Framework*

AIX supports the AIX Cryptographic Framework (ACF). This framework is implemented by the AIX kernel and allows applications access to cryptographic hardware and software supported by the kernel while at the same time isolating applications from the cryptographic hardware and software. In the evaluated configuration, IBM's CLiC software is supported by ACF.

#### *5.2.1.13 Mandatory access control (LAS mode only)*

LAS mode provides full mandatory access control (MAC) for all objects on the system. Every file, directory, IPC object, and process on the system is given a sensitivity label (SL) which cannot be modified by an unprivileged process. Each user account is assigned a range of valid SLs, and the user can only operate on the TOE within that range. A process (or user) can only create objects at its current SL, and can only read and write objects subject to the MAC restrictions imposed by the system. It is not possible for unauthorized users to “downgrade” information or to bypass MAC restrictions by any utility or application on the system. Copies of a file or portions of a file, created by any possible means, will always be protected at an SL at least as high as the original file.

#### *5.2.1.14 Mandatory integrity control (LAS mode only)*

LAS mode provides full mandatory integrity control (MIC) for all objects on the system. Every file, directory, IPC object, and process on the system is given an integrity label (TL) which cannot be modified by an unprivileged process. Each user account is assigned a range of valid TLs, and the user can only operate on the TOE within that range. A process

(or user) can only create objects at its current TL, and can only read and write objects subject to the MIC restrictions imposed by the system. It is not possible for unauthorized users to "upgrade" integrity levels associated with data or to bypass MIC restrictions by any utility of application on the system. Copies of a file, or portions of a file, created by any possible means, will always be protected at a TL no greater than that of the original file.

#### *5.2.1.15 Trusted Network (LAS mode only)*

LAS mode provides export and import of labeled data via network interfaces and enforces mandatory access control for network traffic by means of Trusted Network (TN). TN provides two sets of networking rules: network interface and host filtering. Both types of networking rules determine what processing occurs on a packet before its transmission or when it is received. These rules apply sensitivity labels to packets and enforce MAC restrictions on packets according to those labels.

TN network interface rules enforce packet label processing based on the physical network interface of the host. Host rules enforce packet label processing based on the source and destination IP addresses (with network masking allowed) of the packet, the source and destination ports of the request, and the protocol being used. Both types of rules provide several criteria for determining which packets to drop and which to pass.

### 5.2.2 VIOS

#### *5.2.2.1 Identification & authentication*

VIOS provides identification and authentication (I&A) based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by VIOS. VIOS uses a file-based database to store user I&A data.

VIOS supports both local and remote login. Remote login is supported through telnet.

All individual users are assigned a unique user identifier. This user identifier supports individual accountability. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions.

#### *5.2.2.2 Discretionary access control*

VIOS provides DAC between VIOS SCSI device drivers acting on behalf of LPAR partitions as subjects and logical/physical volumes as objects. It also provides DAC between VIOS Ethernet device drivers acting on behalf of groups of LPAR partitions sharing a virtual network and VIOS Ethernet adapter device drivers where one is the subject and the other is the object (the Ethernet packets cannot contain VLAN tags).

#### *5.2.2.3 Role-based access control*

VIOS includes an RBAC mechanism. VIOS RBAC roles are predefined collections of authorizations that can be assigned to users. The VIOS RBAC mechanism is built on the same mechanism used by AIX RBAC except that the role names and abilities are different. All users of VIOS are considered administrative users. Unlike AIX, there is no legacy VIOS RBAC mechanism.

In this document, the VIOS RBAC mechanism is sometimes referred to as VRBAC in order to make a clear distinction between the VIOS RBAC mechanism and the AIX RBAC mechanism when brevity is necessary.

#### *5.2.2.4 Security management*

VIOS uses roles to perform system/security management, but defines a separate set of roles for system management than those used by AIX. Each VIOS role has a set of commands available to it. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users.

# 6 Documentation

The evaluated documentation as outlined in table 4 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

# 7 IT Product Testing

## 7.1 Developer Testing

### 7.1.1 Test configuration

The test configuration of the system was the following:

- System p POWER6 processor
- System p POWER7 processor

The developer test was done on all hardware platforms listed in the ST. The configuration of the software was consistent with the evaluated configuration as the BAS and LAS mode were chosen during installation time, configuring the system to be compliant with the ST requirements.

### 7.1.2 Testing approach

The test plans provided by the sponsor list test cases by groups, which reflects the mix of sources for the test cases. The mapping provided lists the TSF/TSFI the test cases are associated with. The test cases are mapped to the corresponding Functional Specification and HLD. The sponsor uses several different test suites with the following properties:

- The automated test suites cover the general functionality of the TOE. This test suite contains test cases for almost all security relevant system calls exported by the kernel. This kernel testing includes a large set of tests covering different aspects of ACLs and LAS functionality. In addition, almost all security relevant user space applications are tested as well. The testing of user space covers the local user data store. The test suite and the test cases together configure the system automatically to reach predefined initial test condition to ensure reproducibility of the testing. Testing covers positive and negative testing. The automatic tests prepare the test environment, execute the tests and verify the results with the expected results. The conclusion of the verification is returned to the test framework by reporting that the test case passed or failed. The test framework collects all the reported test results and consolidates it for review by the tester. As the test results are provided with plain ASCII text, the tester is immediately able to see whether testing failed.

Detailed logs are maintained to allow the tester to review any fails and analyze the issue.

- VIOS is tested twofold. The manual tests covering the configuration aspects of VIOS trigger different functions through the use of the command line interface. The test cases explain step-by-step the procedure to be executed by the tester. The test description includes instructions to verify for a certain behavior. The document holding the test instructions is also used to record the actual observed behavior and the resulting judgment whether the respective test passed or failed. In addition to the manual testing of the administrative interface, VIOS interfaces provided to other LPARs are tested. The configuration of AIX for FVT testing includes the utilization of VIOS by using SCSI disks and network connectivity from VIOS.

The test setup was done as required by the test suites which is consistent with the evaluated configuration.

### 7.1.3 Testing results

The test results provided by the sponsor were generated on the hardware systems listed above. As described in the testing approach, the test results of all the automated tests are written to files. In addition a log-file for the different test suites reports more details on the flow of the tests. The test results of the few manual tests have been recorded by the sponsor and those results have been presented in separate files.

All test results from all tested platforms show that the expected test results are identical to the actual test results, considering the expected failures stated in the test plan.

### 7.1.4 Test coverage

The functional specification has identified the following different TSFI:

- system calls
- security critical configuration files (TSF databases)
- trusted programs
- network protocols (RIPSO/CIPSO/IPSec/Kerberos/LDAP/NFS)
- cryptographic functionality
- VIOS provided interfaces (administrative interfaces, VSCSI and shared Ethernet)

A mapping provided by the sponsor shows that the tests cover all individual TSFI identified for the TOE. The analysis of the mapping executed by the evaluator as documented in the test case evaluation report on testing shows that also significant details of the TSFI have been tested with the sponsor's testing. This therefore satisfies the requirements for the evaluation, since an exhaustive specification testing is not required as outlined in CEM, paragraph 1496 [2].

### 7.1.5 Test depth

In addition to the mapping to the functional specification, the sponsor provided a mapping of test cases to subsystems of the TOE design. This mapping shows that all subsystems are covered by test cases. Using the TOE design, the coverage of internal interfaces was evident. To show evidence that the internal interfaces have been called, the sponsor

provided a rationale on how these interfaces are tested. In addition, the evaluator used a kernel debugger to verify that certain interface functions are triggered.

### 7.1.6 Conclusion

The evaluator has verified that developer testing was performed on hardware conformant to the ST. Similarly, the versions of the tested software as well as the configuration of the TOE was consistent with the requirements from the ST. The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the sponsor.

The evaluator analyzed the developer testing coverage and the depth of the testing by reviewing all test cases as demonstrated in the test coverage analysis. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification.

The evaluator reviewed the test results provided by the sponsor and found them to be consistent with the test plans.

## 7.2 Evaluator Testing Effort

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

### 7.2.1 Test configuration

The evaluator verified the test systems installed by the developer to ensure they are configured according to the documentation in the security guidance supported by the release notes explaining the evaluated configuration and the test plan. As assessed in the evaluation report on the administrator guidance, the security guidance and the release notes are consistent with the ST. Hence, the evaluator concludes that the evaluator's configuration is consistent with the ST. The test platforms were IBM System p systems with POWER6 and POWER7 processors located at the sponsor labs in India. The exact hardware and software configuration of the test system can be found in evaluator's test plan.

### 7.2.2 Chosen subset size

The evaluator chose to run a significant subset of the developer's tests on a mix of POWER6 and POWER7 machines with the goal of increasing the assurance and trust in the developer's test results, to familiarize himself with the developer's test environment and gain assurance on the reproducibility of the results.

### 7.2.3 Evaluator tests performed

In addition to repeating developer tests, the evaluator devised tests for a subset of the TOE functionality. The tests are listed in the evaluator's test plan. The evaluator has chosen these tests for the following reason:

- Verification of some of the developer's test results by a completely different approach

### 7.2.4 Summary of Evaluator test results

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

The testing were carried out remote with IBM India. The test environment in Austin consisted LPARs running on POWER6 and POWER7 processors.

The TOE operating system was verified by the evaluator according to the information provided during and by the installation process to ensure the correct state of the system. The evaluator used the TOE version as outlined in the ST for testing.

As the VIOS test cases are manual test cases containing all necessary instructions to setup the system, stimulate the appropriate interfaces and instructions on observing the results, the evaluator simply followed these instructions.

The evaluator established a remote session with the developer to observe the developer's testing and to validate that the test results provided by the developer are trustworthy.

All results from the test cases developed by the evaluator were consistent with the expected results.

Both parts of testing, developer and evaluator test cases, check the corresponding function on the external interfaces. The testing covers the functional testing (does the function works as expected with valid data) as well as the error handling (does the function returns the expected error code when invalid data was supplied).

## 7.3 Evaluator Penetration Testing

The evaluator exercised the following interfaces during penetration testing:

- AIX Systemcalls
- VIOS Commandline
- The TOE's use of perl

The TOE finally withstood the penetration efforts of the evaluator.

# 8 Evaluated Configuration

This certification covers the following configurations of the TOE:

IBM AIX 7 for POWER V7.1 Technology level 7100-00-03 with optional IBM Virtual I/O Server V2.2 including ifixes shipped as part of PRPQ P91209 (e.g. table 3).

# 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.

The following guidance specific for the technology was used: For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

The assurance refinements outlined in the PP and thus in the Security Target were followed in the course of the evaluation of the TOE.

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 with OSPP Extended Packages [7]:
  - General Purpose Cryptography, Version 2.0, 28 May 2010,
  - Integrity Verification , Version 2.0, 28 May 2010,
  - Virtualization, Version 2.0, 28 May 2010,
  - Advanced Management, Version 2.0, 28 May 2010,
  - Labeled Security, Version 2.0, 28 May 2010
- 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 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 rating of the strength of functions does not include the crypto algorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

| Algorithm | Key length | Intended purpose | Implementation standard |
|---|---|---|---|
| RSA | 1024, 2048 | generation and verification of digital signatures | [FIPS186-3], [PKCS1] |
| DSA | L=1024, N=160 bits | generation and verification of digital signatures | [FIPS186-3] |
| TDES with block chaining modes: CBC and CTR | 168 | IPsec, Kerberos, EFS using CLiC, ACF using CLiC | [SP800-67] |
| AES with block chaining modes: CBC, CCM, CTR, CTS, GCM | 128, 192, 256 | IPsec, Kerberos, EFS using CLiC, ACF using CLiC | [FIPS197] |
| SHA-1, SHA-256, SHA-512,SHA-224, SHA-384 | n/a | Generation of Hashes | FIPS PUB 180-3 |

**Tabelle 4: Cryptographic Functions**

## 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 Product specific Acronyms

| | |
|---|---|
| ACE | Access Control Entry |
| ACF | AIX Cryptographic Framework |
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| AIX | Advanced Interactive Executive |
| AIXC | AIX Classic |
| ANSI | American National Standards Institute |
| API | Application Programming Interface |
| BAS | Basic AIX Security |
| CBC | Cipher-Block Chaining |
| CBC-MAC | Cipher-Block Chaining Message Authentication Code |
| CC | Common Criteria |
| CC | Common Criteria for Information Technology Security Evaluation |
| CCM | Counter with CBC-MAC |
| CDE | Common Desktop Environment |
| CDRFS | CD-ROM File System |
| CD-ROM | Compact Disc Read Only Memory |
| CID | Corral ID |
| CIPSO | Common IP Security Option |
| CliC | IBM CryptoLite for C |
| CM | Configuration Management |
| CTR | Counter |
| CTS | Ciphertext Stealing |
| DAC | Discretionary Access Control |
| DLPAR | Dynamic LPAR |
| DRNG | Deterministic Random Number Generator |
| ECD | Extended Component Definition |
| EFS | Encrypted File System |
| EGID | Effective Group ID |
| EOF | End of File |
| EPS | Effective Privilege Set |
| EUID | Effective User ID |
| FIFO | First In First Out |
| FIPS | Federal Information Processing Standard |

| | |
|---|---|
| FIV | File Integrity Verification |
| FPR | Floating Point Register |
| FSF | File Security Flag |
| FSO | File System Object |
| FSP | Functional Specification |
| FTP | File Transfer Protocol |
| GA | General Availability |
| GCM | Galois/Counter Mode |
| GID | Group ID |
| GMAC | Galois Message Authentication Code |
| GPR | General Purpose Register |
| GSKit | IBM Global Security Kit |
| HLD | High Level Design |
| HTML | Hypertext Markup Language |
| I&A | Identification and Authentication |
| ID | Identification |
| IEC | International Electrotechnical Commission |
| IEEE | Once known as the Institute of Electrical and Electronics Engineers |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPC | Inter-Process Communication |
| Ipsec | Internet Protocol Security (a.k.a. IPSEC) |
| IPSO | Internet Protocol Security Option |
| ISO | International Standards Organization |
| ISSO | Information System Security Officer |
| JFS | Journaled File System |
| JFS2 | JFS version 2 |
| KAT | Kernel Authorization Table |
| KCT | Kernel Privileged Command Table |
| KDC | Key Distribution Center |
| KDT | Kernel Privileged Device Table |
| KRT | Kernel Role Table |
| LAS | Labeled AIX Security |
| LDAP | Lightweight Directory Access Protocol |
| LFS | Logical File System |

| | |
|---|---|
| LPAR | Logical Partition |
| LPP | Licensed Product Package |
| LPS | Limiting Privilege Set |
| MAC | Mandatory Access Control |
| MPS | Maximum Privilege Set |
| NAS | IBM Network Authentication Service |
| NFS | Network File System |
| NIM | Network Install Manager |
| NPTRNG | Non-Physical True Random Number Generator |
| NVRAM | Non-Volatile Random Access Memory |
| OID | Object Identification |
| OR | Observation Report |
| OSP | Organizational Security Policy |
| PDF | Portable Data Format |
| PID | Process Identifier |
| PROCFS | Process File System |
| PRPQ | Programming Request for Price Quote |
| PTF | Program Temporary Fix |
| RAID | Redundant Array of Independent Disks |
| RAM | Random Access Memory |
| RBAC | Role-Based Access Control |
| RIPSO | Revised IP Security Option |
| RNG | Random Number Generator |
| RPC | Remote Procedure Call |
| RSH | Remote Shell |
| RTAS | Run-Time Abstraction Layer |
| SA | System Administrator |
| SCSI | Small Computer System Interface |
| SED | Stack Execution Disable |
| SEM | Superuser Emulation Mode |
| SHA | Secure Hash Algorithm |
| SL | Sensitivity Label |
| SMIT | System Management Interface Tool |
| SO | System Operator |
| SPECFS | Special File System |

| | |
|---|---|
| SSF | System Security Flag |
| SSL | Secure Sockets Layer |
| SysV | UNIX System V |
| TCB | Trusted Computing Base |
| TCP | Transmission Control Protocol |
| TDES | Triple Data Encryption Standard |
| TDS | IBM Tivoli Directory Server |
| TID | Thread Identifier |
| TL | Integrity Label |
| TN | Trusted Network |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSD | Trusted Signature Database |
| TSF | TOE Security Functionality |
| TSP | TOE Security Policy |
| UDFS | Universal Data Standard File System |
| UDP | User Datagram Protocol |
| UID | User ID |
| VFS | Virtual File System |
| VIOS | Virtual Input/Output Server |
| VLAN | Virtual Local Area Network |
| VMM | Virtual Memory Manager |
| VRBAC | VIOS RBAC |
| WPAR | Workload Partition |

## 12.3 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-0711-2012, Version 1.8, 2012-08-15, IBM AIX 7 for POWER V7.1 Technology level7100-00-03 with optional IBM Virtual I/O Server V2.2 Security Target with BSI OSPP Compliance, Chapman & Siegert

[7] Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
OSPP Extended Package – General Purpose Cryptography, Version 2.0, 28 May 2010,
OSPP Extended Package – Integrity Verification , Version 2.0, 28 May 2010,
OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010,
OSPP Extended Package – Advanced Management, Version 2.0, 28 May 2010,
OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010

[8] Evaluation Technical Report, Version 6, 2012-08-16, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[9] AIX Version 7.1 Release Notes, Version: GI11-9815-01, Date: 2012-08-06

[8] specifically

- AIS 20, Version 1, 2. Dezember 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

# 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<br>APE_OBJ.2 Security objectives |
| | APE_ECD.1 Extended components definition |
| | APE_REQ.1 Stated security requirements<br>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<br>ASE_OBJ.2 Security objectives |
| | ASE_ECD.1 Extended components definition |
| | ASE_REQ.1 Stated security requirements<br>ASE_REQ.2 Derived security requirements |
| | ASE_TSS.1 TOE summary specification<br>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<br>ADV_FSP.2 Security-enforcing functional specification<br>ADV_FSP.3 Functional specification with complete summary<br>ADV_FSP.4 Complete functional specification<br>ADV_FSP.5 Complete semi-formal functional specification with additional error information<br>ADV_FSP.6 Complete semi-formal functional specification with additional formal specification |
| | ADV_IMP.1 Implementation representation of the TSF<br>ADV_IMP.2 Implementation of the TSF |
| | ADV_INT.1 Well-structured subset of TSF internals<br>ADV_INT.2 Well-structured internals<br>ADV_INT.3 Minimally complex internals |
| | ADV_SPM.1 Formal TOE security policy model |
| | ADV_TDS.1 Basic design<br>ADV_TDS.2 Architectural design<br>ADV_TDS.3 Basic modular design<br>ADV_TDS.4 Semiformal modular design<br>ADV_TDS.5 Complete semiformal modular design<br>ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation |

| Assurance Class | Assurance Components |
|---|---|
| AGD:<br>Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life cycle support | ALC_CMC.1 Labelling of the TOE<br>ALC_CMC.2 Use of a CM system<br>ALC_CMC.3 Authorisation controls<br>ALC_CMC.4 Production support, acceptance procedures and automation<br>ALC_CMC.5 Advanced support |
| | ALC_CMS.1 TOE CM coverage<br>ALC_CMS.2 Parts of the TOE CM coverage<br>ALC_CMS.3 Implementation representation CM coverage<br>ALC_CMS.4 Problem tracking CM coverage<br>ALC_CMS.5 Development tools CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures<br>ALC_DVS.2 Sufficiency of security measures |
| | ALC_FLR.1 Basic flaw remediation<br>ALC_FLR.2 Flaw reporting procedures<br>ALC_FLR.3 Systematic flaw remediation |
| | ALC_LCD.1 Developer defined life-cycle model<br>ALC_LCD.2 Measurable life-cycle model |
| | ALC_TAT.1 Well-defined development tools<br>ALC_TAT.2 Compliance with implementation standards<br>ALC_TAT.3 Compliance with implementation standards - all parts |
| ATE: Tests | ATE_COV.1 Evidence of coverage<br>ATE_COV.2 Analysis of coverage<br>ATE_COV.3 Rigorous analysis of coverage |
| | ATE_DPT.1 Testing: basic design<br>ATE_DPT.2 Testing: security enforcing modules<br>ATE_DPT.3 Testing: modular design<br>ATE_DPT.4 Testing: implementation representation |
| | ATE_FUN.1 Functional testing<br>ATE_FUN.2 Ordered functional testing |
| | ATE_IND.1 Independent testing – conformance<br>ATE_IND.2 Independent testing – sample<br>ATE_IND.3 Independent testing – complete |
| AVA: Vulnerability assessment | AVA_VAN.1 Vulnerability survey<br>AVA_VAN.2 Vulnerability analysis<br>AVA_VAN.3 Focused vulnerability analysis<br>AVA_VAN.4 Methodical vulnerability analysis<br>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.