Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0461-2008

for

AIX 6 version 6100-00-02 with optional Virtual I/O Server (VIOS) version 1.5

from

International Business Machines

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-0461-2008

Operating System

AIX 6 version 6100-00-02 with optional Virtual I/O Server (VIOS)
version 1.5

from	International Business Machines
PP Conformance:	- Labelled Security Protection Profile (LSPP), Version 1.b, 8 October 1999 - Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999 - Role-Based Access Control Protection Profile, Version 1.0, July 30, 1998
Functionality:	PP conformant plus product specific extensions; Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

Common Criteria Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 15 May 2008
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Abteilungspräsident

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 AIX 6 version 6100-00-02 with optional Virtual I/O Server (VIOS) version 1.5 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0385-2006. Specific results from the evaluation process BSI-DSZ-CC-0385-2006 were re-used.

The evaluation of the product AIX 6 version 6100-00-02 with optional Virtual I/O Server (VIOS) version 1.5 was conducted by atsec information security GmbH. The evaluation was completed on 30 April 2008. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: International Business Machines

The product was developed by: International Business Machines

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

4 Validity of the certification result

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

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

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

5 Publication

The product AIX 6 version 6100-00-02 with optional Virtual I/O Server (VIOS) version 1.5 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// 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] International Business Machines
11501 Burnet Road
Austin TX 78758-3400
USA

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the operating system IBM AIX 6 for POWER V6.1 Technology level 6100-00-02 with optional IBM Virtual I/O Server version 1.5 (also called AIX 6.1 hereafter).

AIX is a general purpose, multi-user, multi-tasking operating system. It is compliant with all major international standards for UNIX systems, such as the POSIX standards, X/Open XPG 4, Spec 1170, and FIPS Pub 180. 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.

In LSPP mode, the TOE enforces MAC, MIC, DAC and TCB control policies to implement security goals, such as confidentiality, integrity, and accountability. LSPP mode can operate in a network or stand-alone configuration. In a network configuration, LSPP 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 p5 and POWER6 servers running the TOE.

The TOE Security Functions (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 this 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.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles

- Labelled Security Protection Profile (LSPP), Version 1.b, 8 October 1999 [8]
- Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999 [9]
- Role-Based Access Control Protection Profile, Version 1.0, July 30, 1998 [10].

The TOE Security Assurance Requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [3], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by by ALC_FLR.3 - Systematic Flaw Remediation .

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.5.

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

TOE Security Function	Addressed issue
IA	Identification and Authentication
AU	Auditing

TOE Security Function	Addressed issue
DA	Discretionary Access Control
WP	Workload Partitions
RA	Role-Based Access
PV	Privileges
AZ	Authorizations
MAC	Mandatory Access Control
TN	Networking
MIC	Mandatory Integrity Control
OR	Object Reuse
SM	Security Management
TP	TSF Protection

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.2.

The claimed TOE's strength of functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 5.3 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.

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:

AIX 6 version 6100-00-02 with optional Virtual I/O Server (VIOS) version 1.5

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	IBM AIX 6 for POWER V6.1 with Recommended Technology Package 6100-00-02	Program Number 5765-G63	CD-ROM
2	SW	Virtual I/O Server (VIOS) contained in IBM Advanced Power, Virtualization Version 1.5	Program Number 5765-G30	CD-ROM

No	Type	Identifier	Release	Form of Delivery
3	DOC	Technical Reference: Communications, Volume 1	First Edition November 2007	PDF
4	DOC	Technical Reference: Communications, Volume 2	First Edition November 2007	PDF
5	DOC	Commands Reference, Volume 1	First Edition November 2007	PDF
6	DOC	Commands Reference, Volume 2	First Edition November 2007	PDF
7	DOC	Commands Reference, Volume 3	First Edition November 2007	PDF
8	DOC	Commands Reference, Volume 4	First Edition November 2007	PDF
9	DOC	Commands Reference, Volume 5	First Edition November 2007	PDF
10	DOC	Commands Reference, Volume 6	First Edition November 2007	PDF
11	DOC	Diagnostic Information for Multiple Bus Systems	5.3, December 2004	PDF
12	DOC	Files Reference	First Edition November 2007	PDF
13	DOC	General Programming Concepts: Writing and Debugging Programs	First Edition November 2007	PDF
14	DOC	Operating system and device management	First Edition November 2007	PDF
15	DOC	README addendunm to the AIX guidance	nil	PDF
16	DOC	AIX Version 6.1: Security	First Edition November 2007	PDF
17	DOC	Networks and Communications Management	First Edition November 2007	PDF
18	DOC	AIX 6.1 Technical Reference: Base Operating System and Extensions, Volume 1	First Edition November 2007	PDF

No	Type	Identifier	Release	Form of Delivery
19	DOC	AIX 6.1 Technical Reference: Base Operating System and Extensions, Volume 2	First Edition November 2007	PDF
20	DOC	Using the Virtual I/O Server	Sixth Edition, February 2006	PDF
21	DOC	IBM Workload Partitions for AIX	First Edition November 2007	PDF

Table 2: Deliverables of the TOE

The Licensed Product Packages (LPPs) / File Sets which are allowed to be installed in the evaluated configuration of the TOE are defined in the Security Target [6], chapter 2.3.

The TOE documentation is supplied on CD-ROM.

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:

- Discretionary Access Control (DAC) Policy,
- Mandatory Access Control (MAC) Policy,
- Mandatory Integrity Control (MIC) Policy,
- Authorizations and Privilege Policy,
- Role-Based Access Control Policy;
- Trusted Computing Base (TCB) Protection Policy,
- Identification and Authentication Policy,
- IP Filter Control Policy,
- Auditing Policy,
- Workload Partitions Policy.

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself, for example amongst others the assumptions A.KERB_KEY, A.KERB_PROTECT or A.LDAP_PROTECT (for more environmental aspects please refer to the Security Target [6], chapter 3).

All those environmental aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.ADMIN, OE.CREDEN, OE.HW_SEP, OE.INFO_PROTECT, OE.INSTALL, OE.MAINTENANCE, OE.PHYSICAL, OE.RECOVER, OE.SERIAL_LOGIN and OE.SOFTWARE_IN. The following security objectives apply in environments where specific threats to networked systems need to be countered. (Either physical protection measures or cryptographic controls may be applied

to achieve this objective, but they are not part of the TOE): OE.KERB_BIND, OE.KERB_KEY, OE.KERB_PROTECT, OE.LDAP_PROTECT, OE.PROTECT and OE.RSA_KEY. If the TOE is running on underlying machines that have more than one logical partition configured, the objective OE.LPAR applies. Details can be found in the Security Target [2] chapter 4.2.

5 Architectural Information

General overview of AIX

The target of evaluation (TOE) is the operating system AIX 6.1 with technology package 6100-00-02.

AIX is a general purpose, multi-user, multi-tasking operating system. It is compliant with all major international standards for UNIX systems, such as the POSIX standards, Spec 1170, and FIPS Pub 180. 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.

The evaluated configuration of AIX with the above mentioned technology package consists of a distributed, closed network of high-end, mid-range and lowend IBM System p5 servers running the evaluated version of AIX. All servers complying with the definition of System p5 POWER5 and POWER5+ as well as System p5 POWER6 with hardware components as defined in the Security Target are covered by the evaluation.

The network links and cabling are assumed to be physically protected against eavesdropping and tampering. All hosts within the network must run the evaluated version of the TOE software and must be configured in accordance with the configuration resulting from the initial installation the requirements as described in the guidance documentation.

The TOE Security Functions (TSF) provided by AIX consists of those parts that run in kernel mode plus some defined trusted processes. These together 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.

The hardware and the BootProm firmware are considered not to be part of the TOE but part of the TOE environment.

The TOE includes installation from CDROM and from the network. The TOE includes standard networking applications, such as ftp, rlogin, rsh and NFS. Configuration of those network applications has to be performed in accordance with the guidance provided for LSPP/EAL4+ and CAPP/EAL4+ conformant configuration.

The TOE in the LSPP mode does not include the X-Window graphical interface and X-Window applications. System administration tools include the smitty nongraphical system management tool. In the CAPP mode, X-Windows is allowed to be used.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. No HTTP server is included in the evaluated configuration.

Trusted AIX extents the standard AIX implementation with additional access control mechanisms: discretionary access control (DAC), mandatory access control (MAC),

mandatory integrity control (MIC), trusted computing base (TCB), trusted networking (TN), privileges (PV), authorization (AZ) which are used to implement a role model. This extension consists of a kernel extension for the implementation and enforcement of the access control logic as well as user space tools to manage these mechanisms.

Workload partitioning (WPAR) is provided to allow the definition of process containers which are isolated from each other's operation. WPARs provide the following separation functionality:

- Processes in different containers cannot communicate with each other through IPC,
- File system separation is provided,
- Controlling facility is provided which allows device files to be selectively enabled for different WPARs, and
- Network address isolation.

General overview of VIOS

In addition to the AIX OS, VIOS is part of the TOE as well to provide access to shared SCSI and Ethernet resources.

Conceptually, VIOS resides as a layer between the AIX OS and the physical hardware. Access to the shared resources is restricted based on the VIOS configuration performed by the administrator.

VIOS provides discretionary access control between VIOS SCSI device drivers behavior on behalf of LPAR partitions and logical or physical volumes. In addition, VIOS provides discretionary access control between shared Ethernet device drivers accessing a Hypervisor- maintained virtual LAN and the VIOS Ethernet adapter device driver. A VLAN setup with VLAN tags is not supported.

VIOS defines a separate set of roles compared to AIX for system management. 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. Nevertheless, access to the VIOS management interface must be restricted to authorized administrators.

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. The guidance provides the detailed specification of those files and also defines the access modes for each file.
- VIOS providing access to shared SCSI and Ethernet resources

Security Functions

The security functions that have been evaluated include:

- Identification and Authentication: The TOE requires users to authenticate themselves before they can work with the TOE. The mechanism used for

authentication is a userid/password combination. The system administrator has a variety of configuration parameter he can use to enforce users to select passwords that are hard to guess. In addition the system administrator can define the maximum and minimum life-time of passwords.
Users need to authenticate themselves when they log in but also when they change their identity using the su command or when using network applications like rlogin, telnet, ftp. To protect administrative user IDs, all IDs are subject to the account blocking mechanism enforced after a configured number of consecutive failed login attempts. Root login (CAPP mode) is disabled whereas the root account is disabled in LSPP mode. However, the administrative user IDs with ISSO/SO (LSPP mode) authorization are always allowed to login on the physical console which is considered to reside in a physically protected environment.

- Auditing: The TOE includes the possibility to audit a large number of events. The system administrator can configure which events are audited and is also able to define such events on a per file system object basis, define audit classes and assign them individually to users. This allows for a great flexibility in the configuration of the events that are audited. The evaluated configuration supports bin mode auditing only.
- Discretionary Access Control: The TOE supports discretionary access control for the following different types of objects:
    1. The discretionary access control for file system objects: The discretionary access control for file system objects in the TOE support the standard Unix permission bits extended by access control lists that allow the system administrator and the owner of the file system object to allow or restrict the access to the file system object down to the granularity of a single user.
    2. The discretionary access control for IPC objects: The TOE supports discretionary access control based on Unix permission bits for semaphore, shared memory segments and message queues.

  In addition to the AIX DAC mechanisms, VIOS control access to the shared SCSI and Ethernet resources. This access mediation is subject to the discretion of the administrator.
- Workload partitions (WPAR): The TOE implements an isolation mechanism of processes which are assigned to different process containers called a WPAR. This isolation mechanism covers all mechanisms that allow processes to communicate with each other, including file systems, IPC mechanisms, networking, device file access.
- Role-Based Access Control: Based on the authorizations provided by the TOE, a role model is implemented where one role is assigned zero or more authorizations.
- Mandatory Access Control: The TOE supports MAC for the objects listed for DAC.
- Mandatory Integrity Control: The TOE supports MIC for the objects listed for DAC.
- Trusted Networking: The TOE supports MAC rule enforcement upon network connections. In addition, the TOE provides the RIPSO/CIPSO protocols allow the communication of label information to remote systems.
- Privileges: Trusted AIX disassembles the root privilege into a large number of hierarchical privileges. These privileges are to be used to override access control decisions for allowing administrative actions.

- Authorizations: The user space is able to implement authorization checks to verify whether a calling user bears a particular authorization. These authorizations are hierarchical pendants to privileges in user space. Authorizations are used to implement a role mechanism.
- Object Reuse: The TOE ensures that objects are cleared before they are reassigned to and reused by other subjects. This applies to memory and file system objects as well as to a number of other objects that could transmit information a user might not want to be transmitted to other users.
- System management: The AIX part of the TOE supports the following: System administrator and normal users. Additional privileges that exist within the TOE are not used in the evaluated configuration. System management within the TOE is restricted to the system administrator. He may either use the commands provided for system management or the “smitty” tool, which provides a non-graphical interface. The tool will generate scripts using the system management commands. VIOS provides support for different roles for administrative purposes. As only trusted administrators are allowed to access the management interface of VIOS, these roles are provided for convenience for a group of administrators.
- TOE Protection: The TOE protects itself from tampering by untrusted subjects in a variety of ways. The kernel operates in its own protected address space, which can not be modified or read by untrusted processes. The kernel also prohibits any direct access of untrusted processes to hardware. All non-kernel processes have to use the system call interface to get access to objects in the file system, inter-process communication objects or network objects. The kernel controls access to those objects based on the access control policy for those objects and the access rights defined for the individual users. There is also a number of system calls where the use is restricted to the system administrator. Other system calls have specific parameters that are restricted to system administrators. In addition the TOE uses trusted processes which run with system administrator privileges to implement some of the TOE security functions. Those trusted processes are separated by the kernel from untrusted processes. Also the configuration files used by the TSF are protected by the access control functions of the TOE from unauthorized access by untrusted users.

6 Documentation

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

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

7 IT Product Testing

7.1 Developer Testing

Test configuration

The test configuration of the system was the following:

- P5 570 9117-570 (POWER6 processor)

- P5 595 9119-595 (POWER5 processor)

The developer test was done on all hardware platforms listed in the ST [6]. The configuration of the software was consistent with the evaluated configuration as the CAPP and LSPP mode were chosen during installation time, configuring the system to be compliant with the ST requirements.

Test coverage and depth

The functional specification has identified the following different TSFI:

- system calls
- security critical configuration files (TSF databases)
- trusted programs
- network protocols (RIPSO/CIPSO)
- 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.

In addition to the mapping to the functional specification, the sponsor provided a mapping of test cases to subsystems of the high-level design. This mapping shows that all subsystems are covered by test cases. Using the high-level 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.

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.
- VIOS is tested twofold. The manual tests covering the configuration aspects of VIOS trigger different functions through the use of the command line interface. 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.

Testing results

The test results provided by the sponsor were generated on the hardware systems listed above.

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.

7.2 Evaluator Testing

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 platform was an IBM System p5 p570 with a POWER6 processor located at the sponsor labs in Austin, Texas.

Chosen subset size

Due to the evaluator's experience gained during recent reevaluations of AIX and the general test suite having not being changed, the evaluator decided to observe the developer testing while they were conducted.

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 reasons:

- The test cases cover aspects not included in the developer testing (MAC edge conditions, DAC mechanisms interaction, validation of evaluated configuration enforcement).
- The testing of the domain separation gives additional assurance for the functional verification and can also be used for the vulnerability analysis.
- As the sponsor-supplied test cases already cover the TOE in a broad sense the evaluator has devised a set of test cases which have already vulnerability testing aspects included as well (the tests serve a dual purpose which cover the functional verification of aspects and also address vulnerability testing).

The evaluator created several test cases for testing a few functional aspects where the sponsor test cases were not considered by the evaluator to be broad enough. During the evaluator coverage analysis of the test cases provided by the sponsor, the evaluator gained confidence in the sponsor testing effort and the depth of test coverage in the sponsor supplied test cases.

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.

For testing, the developer used several test cases from the VIOS test suite. All of them are independent from each other. Due to the fact that the current evaluation is a reevaluation and the evaluator already assessed the FVT test suite (which covers almost all security enforcing functions) several times, the evaluator chose to concentrate his efforts on new functionality. In addition, the evaluator worked closely with the developer's test team which allowed him to supervise the developer's testing effort.

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.

All developer testing was observed by the evaluator to validate that the test results provided by the developer are trustworthy.

The limited number of test cases created by the evaluator are due to the fact that the available test cases cover almost all different aspects of the corresponding security enforcing function (different options, different setups, etc.) which is not required by the CC as an exhaustive testing is not required.

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 has devised a set of penetration tests based on the developer's vulnerability analysis and based on the evaluator's knowledge of the TOE gained by the other evaluation activities. All penetration tests have been designed to require only a low attack potential as defined in AVA_VLA.2. The evaluator conducted those tests and did not find any test that resulted in a penetration of the TOE with low attack potential. Also the vulnerability analysis did not identify any vulnerability that could be exploited with low attack potential. Therefore the evaluator has determined as a result of his activities that the TOE is resistant against attacks with low attack potential.

8 Evaluated Configuration

For setting up / configuring the TOE all guidance documents especially the documents listed in table 2 have to be followed.

This certification covers the following configurations of the TOE:

- Either the CAPP installation mode or the LSPP installation mode must be selected during installation time.
- AIX 6.1 supports the use of IPv4 and IPv6.
- Only 64 bit architectures are included.
- Web Based Systems Management (WebSM) is not included.
- Both network (NIM, Network Install Manager) and CD installations are supported.
- Only the default mechanism for identification and authentication and, in CAPP mode only, the LDAP authentication method configured for "UNIX-type" authentication with an SSL connection are included. Support for other authentication options, e.g.,smartcard authentication, is not included in the evaluation configuration.
- If the system console is used, it must be connect directly to the workstation and afforded the same physical protection as the workstation.
- AIX 6.1 provides both a native and a Sys5 print system. In LSPP mode, only Sys5 is supported in the evaluated configuration, as it implements the labeling requirements from LSPP, and only single-level printers are supported.

- LSPP Mode Only: System security flags (a.k.a. kernel security flags) need to be configured as identified in section 6.2.14.1).
- The system must be configured to disable remote access for an individual user after five consecutively failed login attempts have occurred for this user.
- If in CAPP mode and if a windowing environment is used, the CDE file set must be selected at installation time.
- CLiC is included in the evaluated configuration.
- Dynamic Partitioning (Dynamic LPAR, DLPAR) is not supported in the evaluated configuration, i.e. the dynamic (de-) allocation of resources to a partition during operations is not allowed and must be prevented by organizational means in the IT environment.

If the product is configured with more than one TOE server, they are linked by LANs, which may be joined by bridges/routers or by TOE workstations which act as routers/gateways or they connect using the Virtual Input/Output Server (VIOS).

If other systems are connected to the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE.

9 Results of the Evaluation

9.1 CC specific results

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

The evaluation methodology CEM [2] was used for those components used up to EAL4 [4] (AIS 34).

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

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The component
  ALC_FLR.3 - Systematic Flaw Remediation
  augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0385-2006, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the following functionality: Workload Partitions, Role Based Access Control, Trusted Execution, Encrypted File Systems, Multi-level security and D-LPAR.

The evaluation has confirmed:

- for PP Conformance
  - Labelled Security Protection Profile (LSPP), Version 1.b, 8 October 1999 [8]
  - Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999 [9]
  - Role-Based Access Control Protection Profile, Version 1.0, July 30, 1998 [10]

- for the functionality: PP conformant plus product specific extensions; Common Criteria Part 2 extended
- for the assurance: Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
- The following TOE Security Functions fulfil the claimed Strength of Function : medium
  SF IA.1 (User Identification and Authentication
  Data Management)

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 cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for all security functions implementing Security Functional Requirements from the FCS class of Common Criteria part 2.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

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

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, Version 2.3, August 2005

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0461-2008, Release 1.3, 2008-04-07, "IBM AIX 6 for POWER V6.1 Technology level 6100-00-02 with optional IBM Virtual I/O Server Security Target for CAPP, LSPP, and RBACPP Compliance", IBM Corporation

[7] Evaluation Technical Report, Release 2, 2008-04-30, atsec information security GmbH (confidential document)

[8] Labelled Security Protection Profile (LSPP), Version 1.b, 8 October 1999

[9] Controlled Accessy Protection Profile (CAPP), Version 1.d, 8 October 1999

[10] Role-Based Access Control Protection Profile, Version 1.0, July 30, 1998

[11] Technical Reference: Communications, Volume 1, commtrf1.pdf, First Edition November 2007

[12] Technical Reference: Communications, Volume 2, commtrf2.pdf, First Edition November 2007

[13] Commands Reference, Volume 1, aixcmds1.pdf, First Edition November 2007

[14] Commands Reference, Volume 2, aixcmds2.pdf, First Edition November 2007

[15] Commands Reference, Volume 3, aixcmds3.pdf, First Edition November 2007

[16] Commands Reference, Volume 4, aixcmds4.pdf, First Edition November 2007

---

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document resp. CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[17] Commands Reference, Volume 5, aixcmds5.pdf, First Edition November 2007

[18] Commands Reference, Volume 6, aixcmds6.pdf, First Edition November 2007

[19] Diagnostic Information for Multiple Bus Systems, 380509.pdf, Release 5.3, December 2004

[20] Files Reference, aixfiles.pdf, First Edition November 2007

[21] General Programming Concepts: Writing and Debugging Programs, genprogc.pdf, First Edition November 2007

[22] Operating system and device management, baseadmndita.pdf, First Edition November 2007

[23] README addendum to the AIX guidance, guidance_610.pdf

[24] AIX Version 6.1: Security, security.pdf, First Edition November 2007

[25] Networks and Communications Management, commadmndita.pdf, First Edition November 2007

[26] AIX 6.1 Technical Reference: Base Operating System and Extensions, Volume 1, basetrf1.pdf, First Edition November 2007

[27] AIX 6.1 Technical Reference: Base Operating System and Extensions, Volume 2, basetrf2.pdf, First Edition November 2007

[28] Using the Virtual I/O Server, iphb1.pdf, Sixth Edition, February 2006

[29] IBM Workload Partitions for AIX, wpar.pdf, First Edition November 2007

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA. 2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.