Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0472-2008

for

IBM z/VM
Version 5 Release 3

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-0472-2008

IBM z/VM
Version 5 Release 3

from	IBM Corporation
PP Conformance:	- Controlled Access Protection Profile, Version 1.d, Information Systems Security Organization, 1999-10-08 - Labeled Security Protection Profile, Version 1.b, Information Systems Security Organization, 1999-10-08
Functionality:	PP conformant plus product specific extensions
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

Common Criteria Recognition 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 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product 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, 28 July 2008

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Irmela Ruhrmann
Head of Division

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 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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for 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 Assurance 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.

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 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 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 Recognition 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 IBM z/VM Version 5 Release 3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0258-2005. Specific results from the evaluation process BSI-DSZ-CC-0258-2005 were re-used.

The evaluation of the product IBM z/VM Version 5 Release 3 was conducted by atsec information security GmbH. The evaluation was completed on 17 July 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: 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.

---

6 Information Technology Security Evaluation Facility

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.

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 IBM z/VM Version 5 Release 3 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] IBM Corporation
2455 South Road P328
Poughkeepsie
NY 12601
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 z/VM Version 5 Release 3 (z/VM V5R3). z/VM is a general-purpose, multi-user, multi-tasking operating system designed for enterprise computing systems. z/VM can be used by multiple users simultaneously to perform a variety of functions requiring controlled, separated access to the information stored on the system.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles Controlled Access Protection Profile, Version 1.d, Information Systems Security Organization, 1999-10-08 and Labeled Security Protection Profile, Version 1.b, Information Systems Security Organization, 1999-10-08 [10] [11].

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.2 (Flaw reporting procedures).

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.3.

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

TOE Security Function	Addressed issue
F.AU	Audit trail for security relevant events The TOE provides an audit capability that allows generating audit records for security critical events. RACF (Resource Access Control Facility) provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access the resource. The audit records generated by RACF are collected into files residing on disks that are protected from unauthorized modification or deletion by the DAC and (in LSPP mode) MAC mechanism.
F.AC	Discretionary access control (DAC) For implementation of extended DAC rules, RACF provides the capability and flexibility as required by the evaluation compared to the usage of the system. Hence, the evaluated configuration of z/VM includes RACF. A user's authority to access a resource while operating in a RACF-protected system at any time is determined by a combination of these factors: • User's identity and group membership • User's attributes including group-level attributes • User's group authorities • Security classification of the user and the resource profile • Access authority specified in the resource profile

TOE Security Function	Addressed issue
	Mandatory access control (MAC, in LSPP mode) In addition to DAC, z/VM provides Mandatory Access Control (MAC) in LSPP mode, which imposes access restrictions to information based on security classification. Each user and each RACF controlled object can have a security classification specified in its profile. The security classification can be a security level and zero or more security categories. Security labels are maintained separately from privilege classes in RACF. The access control enforced by the TOE ensures that users may only read labelled information if their security label dominates the information's label, and that they may only write to labelled information containers if the container's label dominates the subject's.
F.I&A	Identification & authentication z/VM provides identification and authentication of users by the means of an alphanumeric user ID and a system-encrypted password. The following parts of the TOE perform identification and authentication independently: • Control Program (CP) • Resource Access Control Facility (RACF) For performing identification and authentication, z/VM employs RACF managing resource profiles and user profiles.
F.IP	Interference Protection between virtual machines Operating system failures that occur in virtual machines do not normally affect the z/VM operating system running on the real processor. If the error is isolated to a virtual machine, only that virtual machine fails, and the user can re-IPL without affecting the testing and production work running in other virtual machines. Supported by the underlying processor, the TOE restricts results of software failures (such as program checks) occurring in a virtual machine to this machine, thus not affecting other virtual machines or the CP. Failures of CP that cannot be isolated to a particular virtual machine result in the abnormal termination ("abend") of the Control Program. In the event of such an abend, the system will re-initialize itself, if possible. Special abend code numbers are used to identify the specific reason for the abend.
F.OR	Object re-use The TOE provides a facility clearing protected objects and storage previously used by virtual machines or the TOE itself prior to reassignment to other virtual machines or the TOE. This ensures confidentiality of data maintained either by the TOE or by virtual machines. DASD devices and their derivatives (such as minidisks or temporary disks) are to be cleared manually by the administrator in accordance with the organizational policies. There is additional software support by the IBM Directory Maintenance Facility (DirMaint), which however is not part of this evaluation

TOE Security Function	Addressed issue
F.SM	Security management functions z/VM provides a set of commands and options to adequately manage the TOE's security functions. The TOE recognizes several roles that are able to perform the different management tasks related to the TOE's security: • General security options are managed by security administrators. • Management of MAC attributes is performed by security administrators in LSPP mode. • Management of users and their security attributes is performed by security administrators. • Management of groups can be delegated to group security administrators. • Management of virtual machine definitions is performed by security administrators. • Users are allowed to change their own password, their default group, and their user name. • Users may choose their security label from the range defined in their profile at login time in LSPP mode. • Auditors manage the parameters of the audit system (e.g. list of audited events) and can analyse the audit trail.
F.TP	TOE self protection The z/VM control program enforces integrity of its own domain. No virtual machine can access TOE resources without appropriate authorization. This prevents tampering with TOE resources by untrusted subjects. Supportive to this functionality are hardware implemented facilities, namely the SIE (Start Interpretive Execution) instruction and the Set Address Limit facility provided by the underlying processor. Therefore the hardware and firmware components providing the abstract machine for the TOE are required to be physically protected from unauthorized access.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 2.3.

The claimed TOE's Strength of Functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 1.4 is confirmed.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.3 . Based on these assets the security environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configuration of the TOE as described in chapter 8 of this report or in the Security Target [6], chapter 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 z/VM Version 5 Release 3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
z/VM Version 5 Release 3				
1	SW	z/VM V5R3 SDO, program number 5741-A06	V5R3	Tape / DVD
2	DOC	Program Directory for z/VM V5R3 base	GI10-0782-00	Hardcopy
3	DOC	Program Directory for RACF FL530	GI10-0788-00	Hardcopy
4	DOC	Guide for Automated Installation and Service	GC24-6099-04	Hardcopy
5	DOC	z/VM V5R3 Publications Collection Kit	SK2T-2067-24	DVD / CD-ROM
6	DOC	z/VM V5R3 Secure Configuration Guide as of 2008-02-15 obtained electronically from the IBM Publications Center https://www.vm.ibm.com/security/hcss0b20.pdf	SC24-6139-00	Softcopy
Additional Media				
7	SW	RSU 5302 (PTF UM90235) APAR VM64310 (PTF UM32174) APAR VM64365 (PTF UV61016) obtained electronically from ShopzSeries https://www.ibm.com/software/shopzseries	n/a	Softcopy

Table 2: Deliverables of the TOE

All hardcopies of the guidance documents and the publications DVD are packaged and shipped with the installation media.

All non-softcopy items are shipped together via registered courier to the customer.

To install and configure the TOE such that it matches the evaluated configuration as described in the Security Target, the user has to follow the guidance provided in

- z/VM V5R3 Secure Configuration Guide (SC24-6139-00),

listed as item 6 above. The z/VM V5R3 Secure Configuration Guide can be downloaded from an SSL-secured IBM website.

That document contains references to other guidance documentation contained in item 5, i.e.

- z/VM V5R3 Publications Collection Kit (SK2T-2067-24).

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:

- An *Audit Policy* defined by the SFRs FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.3, FAU_STG.4, FIA_USB.1 and FMT_MTD.1
- An *Identification & Authentication Policy* that is defined by the SFRs FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.7, FIA_USB.1 and FIA_SOS.1.
- A *Mandatory Access Control Policy* defined by the SFRs FDP_ETC.1, FDP_ETC.2, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FDP_ITC.2, FDP_RIP.2, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_REV.1, FPT_RVM.1 and FPT_SEP.1,
- A *Discretionary Access Control Policy* that is defined by the SFRs FDP_ACC.1, FDP_ACF.1, FDP_RIP.2, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_REV.1, FPT_RVM.1 and FPT_SEP.1.
- An *Object Reuse Policy* is defined by the SFRs FDP_RIP.2 and Note 1.
- An *Security Management Policy* is defined by the SFRs FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.3, FAU_STG.4, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1 and FPT_STM.1.
- An *TSF Protection Policy* is defined by the SFRs FPT_RVM.1 and FPT_SEP.1.
- An *Interference Protection Policy* is defined by the SFRs FPT_FLS.1.1, FPT_RVM.1, FPT_SEP.1 and FRU_FLT.1.

In addition to the Security Target the Security Policy of the TOE has been described in a separate Informal TOE security policy model as required by the CC assurance component ADV_SPM.1.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.INSTALL, OE.PHYSICAL, OE.CREDEN, OE.HW_SEP, OE.CLASSIFICATION (LSPP mode only). Details can be found in the Security Target [6] chapter 4.2.

5 Architectural Information

The Target of Evaluation (TOE) is the z/VM virtual machine operating system with the software components as described in chapter 2 above.

z/VM is a general-purpose, multi-user, multi-tasking operating system designed for enterprise computing systems. z/VM can be used by multiple users simultaneously to perform a variety of functions requiring controlled, separated access to the information stored on the system. The TOE provides a virtual machine for each logged in user,

separating the execution domain of each user from other users as defined in the virtual machine definitions stored in the system directory. In addition, the system directory contains access control information for privileged functions (such as codes delivered through the processors DIAGNOSE instruction). In addition to the system directory, RACF is employed to perform access control to resources.

The TOE is seen as one instance of z/VM running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over this abstract machine regardless which software runs inside of virtual machines.

The abstract machine itself is not part of the TOE, but belongs to the TOE environment. Note that although a z/VM instance can be run within a z/VM instance, the evaluated configuration is restricted to one z/VM instance running directly on an abstract machine as defined in chapter 7. A z/VM instance running within a virtual machine is allowed, but this z/VM instance is not in an evaluated configuration (some security functionality may be implemented differently, in particular with respect to the usage of the processor's Start Interpretive Execution (SIE) instruction).

Multiple instances of the TOE may be connected with the instances sharing their RACF database. This can be done by sharing the DASD (direct access storage device) volume keeping the RACF database between the different z/VM instances. Although sharing of one RACF database between z/VM and z/OS is technically feasible, it is explicitly excluded from this evaluation.

The platforms selected for the evaluation consist of IBM products, which are available when the evaluation has been completed and will remain available for a substantial period of time afterwards upon request to IBM.

The TOE security functions (TSF) are provided by the z/VM operating system core (called Control Program – CP), by applications running within virtual machines, and by the Resource Access Control Facility (RACF), which is used by different services as the central instance for identification and authentication and for access control decisions. z/VM provides management functions that allow configuring the TSF and tailor them to the customer's needs.

Some elements have been included in the TOE which do not provide security functions, but run in authorized mode and could therefore, if misbehaved, compromise the TOE. Since these elements are substantial for the operation of many customer environments, they are included as trusted applications within the TOE.

In its evaluated configuration, the TOE allows two modes of operation: LSPP-compliant and CAPP-compliant. In both modes, the same software elements are used. The two modes have different RACF settings with respect to the use of security labels. All other configuration parameters are identical in the two modes.

Major structural units of the TOE

The TOE consists of three major components, i.e. the z/VM Control Program (CP), the Resource Access Control Facility (RACF) component, and the TCP/IP component.

The z/VM Control Program is primarily a real-machine resource manager providing each user with an individual working environment known as a virtual machine. Each virtual machine is a functional equivalent of a real system, sharing the real processor instructions and its functionality, storage, console, and input/output (I/O) device resources.

CP provides connectivity support that allows application programs running within virtual machines to exchange information with each other and to access resources residing on the same z/VM system or on different z/VM systems.

In order to create and maintain these rules (virtual machine definitions), additional management software is employed, that runs outside the CP, but is part of the TOE. Hence, each component of the management software runs within a virtual machine. The following list illustrates, which functionality runs within virtual machines:

- CMS (a general purpose operating system that is employed to run all the following software components within a virtual machine – see section 2.2.1 of the ST [6] for details on the intended usage of CMS in the evaluated configuration)
- RACF (provides authorization and authentication services to CP and to other authorized CMS applications)
- TCP/IP stack application

Note that the TCP/IP stack application contains a Telnet service for users to log on via network and a terminal service (called console) for local log-ins. In particular, this Telnet service receives requests from the network and forwards them into CP using the DIAGNOSE processor instruction. CP generates a virtual console session as a memory object. All outgoing information is sent from the CP back to the Telnet service, which encapsulates the information in the Telnet protocol and sends to the client.

Security Functions Overview

The primary security features of the product that have been subject to evaluation are:

- *Identification and authentication*
- *Discretionary access control*
- *Mandatory access control and support for security labels in LSPP mode*
- *Separation of virtual machines*
- *Audit*
- *Object reuse functionality*
- *Security management*
- *TSF protection*

These primary security features are supported by domain separation and reference mediation, which ensure that the features are always invoked and cannot be bypassed.

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

Test configuration

The TOE is seen as one instance of z/VM running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over this abstract machine regardless which software runs inside of virtual machines. This abstract machine can be provided by one of the following:

- a logical partition of an IBM System z or zSeries machines (PR/SM)
- native mode (no PR/SM logical partition) on z800 and z900

The abstract machine itself is not part of the TOE, but belongs to the TOE environment. It is to be noted that although a z/VM instance can be run within a z/VM instance, the evaluated configuration is restricted to one z/VM instance running directly on an abstract machine as defined above.

Developer tests have been performed on an installation of z/VM V5R3 running within a logical partition of a zSeries 990 server in LPAR mode (GDLTCCC). For all platforms listed as being able to provide the abstract machine for the TOE, the developer performed additional testing to verify that capability. Therefore, all platforms can be considered equivalent with respect to the abstract machine they provide for the TOE.

Independent evaluator tests were executed on the same machine as the developer test.

The test machine was in its evaluated configuration when performing either tests, i.e. all RSU and PTF as required by the ST had been properly installed and all configuration steps as required by the Secure Configuration Guide had been performed prior to testing.

The test machine was configured in LSPP compliant mode in order to be able to run the complete security test suite.

Report on the developer testing effort

TOE test configuration

The developer tests were performed on system GDLTCCC running within a logical partition of a zSeries 990 server in LPAR mode. The TOE had been in its evaluated configuration when developer tests were performed.

Testing approach

The developer designed a specific CC related test suite that contains several test scenarios covering the TOE security functions. The tests performed by the developer directly stimulate the TSFI and observe the TSF behaviour.

All but one test case were automated. Proper verification whether the actual test results match the expected results was already included in the respective test cases.

Amount of developer testing performed

As demonstrated in the developer's test coverage analysis, testing was performed for all TOE security functions. All identified TSFI were used for developer testing, some of them by direct stimulation as part of test cases, some indirectly.

The developer testing was performed to the depth of the high-level design, i.e. the developer test-depth analysis demonstrated that the TOE subsystems CP, RACF, and

TCPIP have been subject to test cases exercising the TSFI and the TSF implemented by those components.

Testing results

The majority of developer test cases passed, i.e. the actual test results matched the expected results. For four of the test cases, the developer testing returned unexpected results, thus formally causing those test cases to fail.

Report on the evaluator testing effort

The following independent testing was performed by the evaluator:

TOE test configuration

The tests were performed on the system GDLTCCC running within a logical partition of a zSeries 990 server. Note that this was the system the developer testing was also performed on. The test system had installed the z/VM Version 5 Release 3, which was displayed after logon. The TOE had been in its evaluated configuration when the evaluator tests were performed.

Testing approach

The evaluator repeated a randomly chosen subset of the developer tests. For each of the test case groups “CP commands”, “RACF commands”, and “DIAGNOSE”, coverage of at least 21% was achieved by the sampling strategy. No SAK test case was repeated.

In addition, the evaluator devised independent test cases to cover the TSFI that are not explicitly but only implicitly triggered by the developer tests. The independent evaluator test cases directly triggered the TELNET Server, the RACF ReportWriter, and the SystemDirectory.

The evaluator covered all TSF by independent test cases.

Testing results

The overall judgment on the results of evaluator testing during the evaluation is that all tests performed passed.

By using developer tests as base for independent testing, the evaluator achieved the same test depth as the developer when repeating a subset of the developer tests. Therefore, the tests performed by the evaluator were at the level of the TOE high-level design.

There were no failed tests that were caused by TOE behaviour different from the expected behaviour or violating requirements stated in ST.

Report on the evaluator penetration testing

The evaluator examined the developer’s vulnerability analysis and also consulted public domain information in order to identify vulnerabilities that would require performing penetration testing based on the developer's analysis.

Apart from the vulnerabilities listed by the developer, the evaluator was not able to identify any other vulnerability[8]. The evaluator considered the rationale provided by the developer as sound and also verified that the calculation of the attack potential for residual

[8]An open PTF labelled as security relevant was assessed by the evaluator when performing the vulnerability analysis. The security problem, i.e. the possibility of a denial-of-service attack, was considered to only have an impact on the availability of the TOE, for which the ST does not contain a claim. Integrity of TOE data is not impacted, since the TOE enters a secure state once the reported problem occurs and requires a restart, which includes a re-initialization of all user data in virtual machines.

vulnerabilities is correct. Since the evaluator is not expected to test for non-exploitable or residual vulnerabilities, no penetration testing based on the developer's vulnerability analysis was performed.

As for the penetration testing based on the evaluator's independent vulnerability analysis the evaluator devised two penetration test cases. Whereas one of the test cases was intended to identify additional interfaces potentially bearing weaknesses, the second test case was intended to explicitly probe for weaknesses of the TELNET server interface. Both tests were performed at the depth of the high-level design probing the TCP/IP subsystem of the TOE.

A portscan was performed from within the same network segment the TOE was located in to eliminate interferences with other active network component. It matches the expected results.

Attempts to deliberately provoke buffer overflows during input of user credentials were performed. The excessive inputs were rejected with error messages, thus matching the expected results.

8 Evaluated Configuration

The Target of Evaluation (TOE) is the IBM z/VM Version 5 Release 3.

The evaluated configuration of the TOE is stated in the ST [6] as follows:

“The Target of Evaluation, IBM z/VM Version 5 Release 3, requires the following software elements to be installed:

- *Conversational Monitor System (CMS) for operating RACF and TCP/IP.*
- *Control Program (CP).*
- *RACF*
- *TCP/IP for z/VM*
- *RSU 5302*
- *PTF UM32174*
- *PTF UV61016*

The TOE is seen as one instance of z/VM running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over this abstract machine regardless which software runs inside of virtual machines. This abstract machine can be provided by one of the following:

- *a logical partition of an IBM zSeries machine (PR/SM)*
- *native mode (no PR/SM logical partition) on z800 and z900*

The abstract machine itself is not part of the TOE, but belongs to the TOE environment. It is to be noted that although a z/VM instance can be run within a z/VM instance, the evaluated configuration is restricted to one z/VM instance running directly on an abstract machine as defined above.”

Guidance documentation

- z/VM Version 5 Release 3 CP Commands and Utilities Reference, SC24-6081-04, Version: -04, June 2007

- z/VM Version 5 Release 3 CP System Messages and Codes, GC24-6119-04, Version: -04, June 2007
- z/VM Version 5 Release 3 CP Planning and Administration, SC24-6083-04, Version: -04, June 2007z/VM Version 5 Release 3 CP Programming Services, SC24-6084-03, Version: -03, June 2007
- z/VM Version 5 Release 3 RACF Security Server Auditor's Guide, SC24-6143-00, Version: -00, June 2007
- z/VM Version 5 Release 3 RACF Security Server Command Language Reference, SC24-6144-00, Version: -00, June 2007
- z/OS Security Server RACF Callable Services, SA22-7691-10, Version: -1, September 2006
- z/VM Version 5 Release 3 RACF Security Server Diagnosis Guide, SC24-6145-00, Version: -00, June 2007
- z/VM Version 5 Release 3 RACF Security Server General User's Guide, SC24-6146-00, Version: -00, June 2007
- z/VM Version 5 Release 3 RACF Security Server Messages and Codes, SC24-6148-00, Version: -0, June 2007
- z/VM Version 5 Release 3 RACF Security Server Macros and Interfaces, SC24-6147-00, Version: -00, June 2007
- z/VM Version 5 Release 3 RACF Security Server Security Administrator's Guide, SC24-6142-00, Version: -00, June 2007
- Secure Configuration Guide IBM z/VM Version 5 release 3, Version: Feb 2008, 15.02.2008
- z/VM Version 5 Release 3 System Operation, SC24-6121-02, Version: -0, June 2007
- z/VM Version 5 Release 3 TCP/IP Diagnosis Guide, GC24-6123-02, Version: -02, June 2007
- z/VM Version 5 Release 3 TCP/IP Messages and Codes, GC24-6124-02, Version: -02, June 2007
- z/VM Version 5 Release 3 TCP/IP Planning and Customization, SC24-6125-03, Version: -03, June 2007
- z/VM Version 5 Release 4 TCP/IP Programmer's Reference, SC24-6126-01, Version: -01, June 2007
- z/Architecture Principle of Operation, SA22-7832-05, Version: -0, April 2007

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 all assurance requirements claimed for the TOE.

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 components ALC_FLR.2 (Flaw reporting procedures) 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-0258-2005, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on an increased assurance level from EAL 3 up to EAL 4 also as the new functionalities

- SSL/TLS switching possibility for telnet sessions
- r_admin interface usable for other virtual machines via IUCV communication channels
- addition of new CP commands
- addition of new DIAGNOSE codes

The evaluation has confirmed:

- PP Conformance: - Controlled Access Protection Profile, Version 1.d, Information Systems Security Organization, 1999-10-08
  - Labeled Security Protection Profile, Version 1.b, Information Systems Security Organization, 1999-10-08 [10][11]
- for the Functionality: PP conformant plus product specific extensions
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.2
- The TOE Security Function F.I&A (Identification and Authentication) fulfil the claimed Strength of Function: medium

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 TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

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

CP Control Program

DAC Discretionary Access Control

DASD Direct Access Storage Device

EAL Evaluation Assurance Level

IPL Initial Program Load

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

MAC Mandatory Access Control

PP Protection Profile

PSW Program Status Word

PR/SM Processor Resource/ Systems Manager

RACF Resource Access Control Facility

SF Security Function

SFP Security Function Policy

SIE Start Interpretive Execution

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

Assets - Information or resources to be protected by the countermeasures of a TOE.

Assignment - The specification of an identified parameter in a component.

Assurance - Grounds for confidence that an entity meets its security objectives.

Attack potential - The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Authentication data - Information used to verify the claimed identity of a user.

Authorised user - A user who may, in accordance with the TSP, perform an operation.

Class - A grouping of families that share a common focus.

Component - The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Connectivity - The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency - A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Element - An indivisible security requirement.

Evaluation - Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL) - A package consisting of assurance

components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority - A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme - The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

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.

External IT entity - Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family - A grouping of components that share security objectives but may differ in emphasis or rigour.

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

Human user - Any person who interacts with the TOE.

Identity - A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal - Expressed in natural language.

Internal communication channel - A communication channel between separated parts of TOE.

Internal TOE transfer - Communicating data between separated parts of the TOE.

Inter-TSF transfers - Communicating data between the TOE and the security functions of other trusted IT products.

Iteration - The use of a component more than once with varying operations.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organisational security policies - One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

Package - A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Product - A package of IT software, firmware and/or hardware, providing functionality designed

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

Reference monitor - The concept of an abstract machine that enforces TOE access control policies.

Reference validation mechanism - An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement - The addition of details to a component.

Role - A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret - Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security attribute - Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

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 Function Policy (SFP) - The security policy enforced by an SF.

Security objective - A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

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

Selection -The specification of one or more items from a list in a component.

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.

System - A specific IT installation, with a particular purpose and operational environment.

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

TOE resource - Anything useable or consumable in the TOE.

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 Functions Interface (TSFI) - A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

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

TOE security policy model- A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control - Communicating data to entities not under control of the TSF.

Trusted channel - A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path - A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

TSF data - Data created

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.

User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data - Data created by and for the user, that does not affect the operation of the TSF.

13 Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[9]

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

[6] Security Target BSI-DSZ-0472-2008 Version 2.6, 10.06.2008, Security Target for IBM z/VM Version 5 Release 3, IBM Corporation

[7] Evaluation Technical Report, Version 2.0, 17.07.08, Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] [ConfCode] Configlist for zVM CP, RACF, and TCPIP components, 17.03.2008, (confidential document)

[9] [ConfDoc] zVM 5.3 Documenation Set, 30.11.2007, (confidential document)

[10] Controlled Access Protection Profile, Version 1.d, Information Systems Security Organization, 1999-10-08

[11] Labeled Security Protection Profile, Version 1.b, Information Systems Security Organization, 1999-10-08

[12] Secure Configuration Guide IBM z/VM Version 5 Release 3, 15.02.08, SC24-6139-00, IBM Corporation (https://www.vm.ibm.com/security/hcss0b20.pdf)

[9] specifically

- AIS 14, Version 1: Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, Stand 24.11.1998
- AIS 19, Version 1: Gliederung des ETR, Stand 12.11.1998
- AIS 32, Version 1: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Stand 02. 07. 2001
- AIS 38, Version 2.0: Reuse of evaluation results, Stand 28 September 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.

This page is intentionally left blank.