



Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0247-2005

for

**IBM z/OS
Version 1, Release 6**

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111



Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik



Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0247-2005

**IBM z/OS
Version 1, Release 6**

from

IBM Corporation



Common Criteria Arrangement

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, Part 1 Version 0.6, Part 2 Version 1.0* extended by CEM supplementation "ALC_FLR – Flaw remediation", Version 1.1, February 2002 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance: **Labeled Security Protection Profile (LSP), Issue 1.b, 08.10.1999 and Controlled Access Protection Profile (CAPP), Issue 1.d, 08.10.1999**

Functionality: **PP conformant plus product specific extensions
Common Criteria Part 2 extended**

Assurance Package: **Common Criteria Part 3 conformant
EAL3 augmented by ADV_SPM.1 (Informal TOE security policy model)
and ALC_FLR.1 (Basic flaw remediation)**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, March 09th, 2005

The President of the Federal Office
for Information Security



Dr. Helmbrecht

L.S.

SOGIS-MRA

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn

Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

The rating of the strength of functions does not include the cryptographic algorithms suitable for encryption and decryption (see BSIG Section 4, Paragraph 3, Clause 2)

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.

Preliminary Remarks

Under the BSIG¹ 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

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

A Certification

1 Specifications of the Certification Procedure

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

- BSIG²
- BSI Certification Ordinance³
- BSI Schedule of Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1⁵
- Common Methodology for IT Security Evaluation (CEM)
 - Part 1, Version 0.6
 - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- CEM supplementation on “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

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 7 July 1992, Bundesgesetzblatt I p. 1230

⁴ Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

⁵ Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

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 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).

2.2 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 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004.

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/OS Version 1, Release 6 has undergone the certification procedure at BSI.

The evaluation of the product IBM z/OS Version 1, Release 6 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)⁶ recognised by BSI.

The developer and sponsor is:

IBM Corporation
2455 South Road
Poughkeepsie NY 12601 - USA

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 09.03.2005.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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

4 Publication

The following Certification Results contain pages B-1 to B-32.

The product IBM z/OS Version 1, Release 6 has been included in the BSI list of the certified products, which is published regularly (see also Internet: <http://www.bsi.bund.de>). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor⁷ of the product. The Certification Report can also be downloaded from the above-mentioned website.

⁷ IBM Corporation
2455 South Road
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.

Contents of the certification results

1	Executive Summary	3
2	Identification of the TOE	12
3	Security Policy	14
4	Assumptions and Clarification of Scope	15
5	Architectural Information	16
6	Documentation	19
7	IT Product Testing	20
8	Evaluated Configuration	22
9	Results of the Evaluation	24
10	Comments/Recommendations	26
11	Annexes	27
12	Security Target	28
13	Definitions	29
14	Bibliography	32

1 Executive Summary

The Target of Evaluation (TOE) is IBM z/OS Version 1, Release 6.

z/OS is a general-purpose, multi-user, multi-tasking operating system for enterprise computing systems running on IBM zSeries mainframe computers. Multiple users can use z/OS simultaneously to perform a variety of functions that require controlled, shared access to the information stored on the system.

The TOE includes software components only and provides LSPP and CAPP compliant security functionality plus product specific extensions. Among these functions are:

- Identification and Authentication
- Discretionary and Mandatory Access Control
- Secure Communication
- Audit
- Object re-use functionality
- Security Management
- TSF Protection

The TOE is one instance of z/OS running on an abstract machine as the sole operating system and exercising full control over this abstract machine. This abstract machine can be provided by

- an IBM zSeries Processor,
- a logical partition of an IBM zSeries Processor (certified version of PR/SM) or
- z/VM (certified version) either running on a zSeries Processor or on a logical partition of PR/SM

For details about the abstract machine please refer to chapter 1.6 of this report.

For more details concerning the software version defining the TOE, the abstract machine the TOE runs on and the user guidance documentation delivered with the TOE please refer to the remainder of this report.

The TOE Security Functional Requirements (SFRs) used in the Security Target are Common Criteria Part 2 extended as shown in the following table:

Security Functional Requirement	Identifier
<i>SFRs from CC Part 2, contained in LSPP/CAPP</i>	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Guarantees of audit data availability
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FDP_ACC.1	Discretionary access control policy
FDP_ACF.1	Discretionary access control functions
FDP_ETC.1	Export of unlabeled user data
FDP_ETC.2	Export of labeled user data
FDP_IFC.1	Mandatory access control policy
FDP_IFF.2	Mandatory access control functions
FDP_ITC.1	Import of unlabeled user data
FDP_ITC.2	Import of labeled user data
FDP_RIP.2	Object residual information protection
FIA_ATD.1	User attribute definition
FIA_SOS.1	Strength of authentication data
FIA_UAU.1	Authentication
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Identification
FIA_USB.1	User-subject binding
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management
FMT_REV.1	Revocation of attributes

Security Functional Requirement	Identifier
FMT_SMR.1	Security management roles
FPT_RVM.1	Reference mediation
FPT_SEP.1	Domain separation
FPT_STM.1	Reliable time stamps
<i>SFRs not in CC Part 2 (Part 2 extended), contained in LSPP/CAPP</i>	
„Note1“ as defined in LSPP/CAPP	Subject Residual Information Protection
<i>SFRs from CC Part 2, not contained in LSPP/CAPP</i>	
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Distribution
FCS_COP.1	Cryptographic Operation
FDP.UTC.1	Basic data exchange confidentiality
FDP.UIT.1	Data exchange integrity
FMT_MSA.2	Secure security attributes
FMT_SMF.1 ⁸	Specification of Management Functions
FPT_TDC.1	Inter-TSF basic TSF data consistency
FTP_ITC.1	Inter-TSF trusted channel

Note that some of the SFRs have been iterated in the Security Target. For details on the iteration and the required security functionality please refer to [7], chapter 5.1.

The IT product IBM z/OS Version 1, Release 6 (for details on the evaluated configuration please refer to chapter 2) was evaluated by atsec information security GmbH. The evaluation was completed on 07.03.2005. The atsec information security GmbH is an evaluation facility (ITSEF)⁹ recognised by BSI.

The developer and sponsor is

IBM Corporation
2455 South Road
Poughkeepsie NY 12601 - USA

⁸ Added because of AIS32, Final Interpretation 065

⁹ Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL3+ (Evaluation Assurance Level 3 augmented).

The assurance level is augmented by: ADV_SPM.1 – Informal TOE security policy model and ALC_FLR.1 – Basic flaw remediation. For the evaluation of the CC component ALC_FLR.1 the mutually recognised CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([5]) was used.

1.2 Functionality

The TOE security functions are:

Identification and authentication: The TOE provides identification and authentication of users by the means of an alphanumeric user ID and a system-encrypted password.

Discretionary access control: The TOE supports access controls that are capable of enforcing access limitations on individual users and data objects. Discretionary access control (DAC) allows individual users to specify how such resources as direct access storage devices (DASDs), tape data sets, and tape volumes that under their control are to be shared. DAC is provided by two mechanisms. The z/OS standard DAC mechanism is used for most protected objects, except for UNIX file system objects, which are protected by the z/OS UNIX DAC mechanism.

Mandatory access control: In addition to DAC, the TOE provides mandatory access control (MAC) in LSPP mode, which imposes access restrictions to information based on security classification. Users and resources can have a security label specified in their profile. Security labels contain a hierarchical classification (security level), which specify the sensitivity (for example: public, internal use, or secret), and zero or more non-hierarchical security categories (for example: PROJECTA or PROJECTB). The access control enforced by the TOE ensures that users can only read labelled information if their security labels dominate the information's label, and that they can only write to labelled information containers if the container's label dominates the subject's, thus implementing the Bell-LaPadula model of information flow control.

Audit: The TOE provides an auditing capability that allows generating audit records for security-critical events. RACF (Resource Access Control Facility) as part of the TOE provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access the resource. Audit records are collected by the System Management Facilities (SMF) into an audit trail, which is protected from unauthorized modification or deletion by the DAC and (in LSPP mode) MAC mechanisms.

Object re-use: The TOE ensures the re-usability of protected objects and storage before making it accessible to further use.

Security management: The TOE provides a set of commands and options to adequately manage the TOE's security functions. Several roles are recognized that are able to perform the different management tasks related to the TOE's security.

Secure communication: z/OS provides means of secure communication between systems sharing the same security policy. In LSPP mode, communication within TOE parts coupled into a sysplex can be multilevel, whereas other communication channels are assigned a single security label. In CAPP mode, no labels are assigned and evaluated for any communication channel. The confidentiality and integrity of network connections are assured by Secure Sockets Layer / Transport Layer Security (SSLv3/TLSv1) or IPsec-encrypted communication (with the Internet Key Exchange / IKE) for TCP/IP connections.

TSF protection: TSF protection is based on several protection mechanisms that are provided by the underlying abstract machine the TOE is executed upon.

Only a brief summary of the security functionality was provided here. For a precise definition of the SF please refer to the Security Target of the TOE ([7], chapter 6)

1.3 Strength of Function

The TOE's strength of function is rated 'SOF-medium' for the authentication function using passwords (refer to [7], chapter 6.2).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

In compliance with LSPP and CAPP all security objectives are derived from OSP. Therefore no threats have been defined in [7].

The TOE has to comply to the following Organisational Security Policies (OSPs). Note that only a summary of the policies is provided here. For the detailed and precise definition refer to [7], chapter 3.4:

P.AUTHORIZED_USERS

Only users who have been authorised to access information within the system may access the system.

P.NEED_TO_KNOW

The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users who have a "need to know" for that information.

P.ACCOUNTABILITY

The users of the system shall be held accountable for their actions within the system.

P.CLASSIFICATION

The system must limit the access to information based on sensitivity and formal clearance of users (LSPP mode only).

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in chapter 2.3.1 and subsequent chapters of the Security Target [7] and are summarised here (please refer to the Security Target for the precise and more detailed description):

- Installation and configuration of the TOE components as detailed in chapter 2 and 6 of this report is required.
- Software outside the TOE components boundary may be added if this software cannot run (i) in supervisor mode, (ii) APF-authorized, (iii) with keys 0 through 7
- Replacement of any element in the ServerPac is not allowed
- The following elements or element components are not to be used:
 - All Bulk Data Transfer (BDT) elements: BDT (FMID HBD6602), BDT File-to-File (FMID JBD6201), and BDT Systems Network Architecture (SNA) NJE (FMID JBD6202)
 - Connection Manager (FMID HCMG110)
 - The Distributed Computing Environment (DCE) component (FMID HRSS190) of the Integrated Security Services element
 - DCE Base Services (FMID HMB3190)
 - The DFS™ Server Message Block (SMB) and DFS DCE-DFS (FMID H0H2360) components of the Distributed File Service element
 - The Enterprise Identity Mapping (FMID HIT7709) component of the Integrated Security Services element
 - Infoprint Server (FMIDs HMOS705, HNET708, and HOPI708)
 - The Integrated Cryptographic Service Facility (ICSF, FMID HCR770A) component of the Cryptographic Services element
 - JES3 (FMID HJS7708)
 - The Lightweight Directory Access Protocol (LDAP) server component (FMIDs HRSL360 and JRSL362) of the Integrated Security Services element

- Managed System Infrastructure for Operations (msys for Operations, FMIDs HPZ8500 and HKYS300)
- The Multiple Virtual Storage / Advanced Program-to-Program Communication (MVS/APPC) component of the BCP (FMID HBB7709)
- The Network Authentication Service component (FMID HSWK360) of the Integrated Security Services element
- Network File System (FMIDs HDZ11US (NFS Server) and HDZ11UC (NFS Client))
- Process Manager (FMID HPMG110)

They have to be either deactivated or to be not configured for use.

- The PassTicket authentication mechanism has not been part of the evaluation and cannot be used in the evaluated configuration.
- The RACF Remote Sharing Facility has not been part of the evaluation and cannot be used in the evaluated configuration.
- The Data Facility Storage Management Subsystem (DFSMS) Object Access Method for content management type applications cannot be used.

1.6 Assumptions about the operating environment

The following assumptions about the technical environment in which the TOE is intended to be used are defined in the ST [7], chapter 2.3.2 and are summarized here:

The TOE can be run either directly, or within a logical partition provided by a certified version of PR/SM, on the z/Architecture as implemented by the following hardware platforms:

- IBM zSeries model z800
- IBM zSeries model z890
- IBM zSeries model z900
- IBM zSeries model z990

In addition, the TOE may run on a virtual machine provided by a certified version of z/VM.

For details on peripherals which can be used with the TOE, while still preserving the security functionality please refer to [7], chapter 2.3.2.

The following constraints concerning the operating environment are made in the Security Target. They are based on the assumptions defined in [7], chapter 3.2. (Please refer to the Security Target for the precise and more detailed definition):

Identifier	Summary
A.LOCATE	Location of TOE processing resources in facilities with controlled access.
A.PROTECT	Protection against physical modification (of TOE hardware and software).
A.MANAGE	Management of the TOE is done by competent individuals.
A.NO_EVIL_ADMIN	Administrative personnel are not careless, wilfully negligent, or hostile.
A.COOP	Authorised users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a co-operating manner.
A.CLEARANCE (LSPP mode only)	Procedures exist for granting users authorization for access to specific security levels.
A.SENSITIVITY (LSPP mode only)	Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (such as printers, tape drives, and disk drives) attached to the TOE, and marking a sensitivity label on all output generated.
A.PEER	Any other system with which the TOE communicates is assumed to be under the same management control and operate under the same security policy constraints.
A.CONNECT	All connections (to peripherals and other systems) not using the secured protocols TLS v1 SSL v3 or IPsec reside within the controlled access facilities. It is assumed that the client chooses SSL v3 or TLS v1 and one of the strong cipher suites as defined the ST, chapter 5.

The following constraints are based on Security Objectives which have to be met by the TOE environment. These objectives are defined in [7], chapter 4.2. (Please refer to the Security Target for the precise and more detailed definition):

Identifier	Summary
OE.INSTALL	The installation, management and operation of the TOE has to be done in a secure manner.

Identifier	Summary
OE.CREDEN	User Authentication Data has to be treated securely.
OE.HW_SEP	The underlying abstract machine has to provide separation mechanisms.

1.7 Disclaimers

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 is called: **IBM z/OS Version 1, Release 6**

The TOE is software only. The following product components represent the TOE:

Software Components:

z/OS Version 1 Release 6, in the “Common Criteria Evaluated Base” version consists of the following tape sets:

- z/OS V1R6 Common Criteria Evaluated Base (IBM program number 5694-A01) with enabled features:
- CBPDO tape with additional service, including RACF APAR OA09052
- IBM Print Services Facility™ Version 3 for z/OS (PSF V3R4, program number 5655-B17)
- Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191).

Guidance Documents:

- Memo to Customers of z/OS V1.6 Common Criteria Configuration
- ServerPac: IYO (Installing Your Order), a custom-built installation manual shipped in printed form.
- z/OS V1R6.0 Planning for Multilevel Security and the Common Criteria (IBM Document number GA22-7509-02) shipped in printed form.
- ServerPac Using the Installation Dialog (Dialog Level 17) (IBM Document number SA22-7815-09) provided on the set of documentation CD-ROMs
- z/OS V1R6.0 Information Roadmap (IBM Document number SA22-7500-07), which contains references to other relevant documents provided on a set of documentation CD-ROMs.
- Additional documents shipped on CD-ROM:
 - z/OS V1R6 Program Directory
 - z/OS V1.6 Collection
 - PSF 3.4 CDROM Kit BOOK
 - PSF 3.4 CDROM Kit PDF
 - PSF V3R4 User's Guide

- Overlay Generation Language/370: User's Guide and Reference
- OGL/370 V1R1.0: Getting Started
- OGL/370 V1R1.0: LPS
- OGL: Command Summary and Quick Reference

3 Security Policy

The TOE implements several policies which are specified in the Security Target by the TOE security functional requirements. Those policies are:

- 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, FIA_SOS.1, FMT_MTD.1, FMT_REV.1, FMT_MTD.1
- Access Control Policies.
A **Mandatory Access Control Policy** defined by the SFRs FDP_IFC.1, FDP_IFF.2, FDP_ETC.1, Note 1, FDP_ITC.1, FDP_ITC.2, FIA_ATD.1, FIA_USB.1, FMT_MSA.1, FMT_REV.1, FPT_TDC.1 and
a **Discretionary Access Control Policy** that is defined by the SFRs FDP_ACC.1, FDP_ACF.1, FDP_ACF.1, FIA_ATD.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_REV.1.
- An **Audit Policy** defined by the SFRs FAU_GEN.1.2, 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, FMT_MTD.1, FMT_MTD.1, FPT_STM.1
- A **Trusted Channel Policy** defined by the SFRs FDP_UCT.1, FDP_UIT.1, FMT_MTD.1, FTP_ITC.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

4.1 Usage assumptions

Based on the personnel and procedural assumptions the following usage conditions exist. Refer to [7], chapter 3.2.2 and 3.2.3 for more details:

- The TOE is managed by competent individuals (A.MANAGE).
- Administrative personnel are not careless, wilfully negligent, or hostile (A.NO_EVIL_ADMIN).
- Users of the TOE are co-operative (A.COOP).

LSP mode only:

- Procedures for granting users authorization for access to specific security levels exist (A.CLEARANCE).
- Procedures for establishing the security level exist (A.SENSITIVITY)

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [7], chapter 3.2.1 and 3.2.4):

- The TOE is located in an access controlled facility (A.LOCATE).
- The TOE (Hardware used by the TOE and the TOE software itself) is protected against physical modification (A.PROTECT).
- Any other system with which the TOE communicates is assumed to be under the same management control and operate under the same security policy constraints. (A.PEER)
- All connections (to peripheral devices and other systems) not using TLSv1, SSLv3 or IPsec reside within the controlled access facilities (A.CONNECT).

Please consider also the requirements for the evaluated configuration specified in chapter 2 and 8 of this report.

4.3 Clarification of scope

No threats to be averted by the TOE environment have been defined in the Security Target [7].

5 Architectural Information

The Target of Evaluation (TOE) is the z/OS operating system with the software components as described in chapter 2 and 8 of this report. z/OS is a general-purpose, multi-user, multi-tasking operating system for enterprise computing systems. Multiple users can use z/OS simultaneously to perform a variety of functions that require controlled, shared access to the information stored on the system.

The TOE is seen as one instance of z/OS running on an abstract machine as the sole operating system and exercising full control over this abstract machine.

This abstract machine can be provided by one of the following:

- an IBM zSeries processor (z800, z890, z900, or z990)
- a logical partition of an IBM zSeries processor (certified version of PR/SM)
- certified version of z/VM on a zSeries processor or on a logical partition of PR/SM

The abstract machine itself is not part of the TOE, rather, it belongs to the TOE environment.

Multiple instances of the TOE may be connected in a basic sysplex or in a parallel sysplex with the instances sharing their RACF database.

The individual TOEs can be run alone or within a network as a set of co-operating hosts, operating under and implementing the same set of security policies.

Transmission Control Protocol/Internet Protocol (TCP/IP) network services, connections, and communication that occur outside of a sysplex are restricted to one security label; that is, each system regards its peers as single-label hosts. Other network communication is disallowed, with the exception of the Job Entry System 2 (JES2) Network Job Entry (NJE) protocol.

Most of the TOE security functions (TSF) are provided by the z/OS operating system Base Control Program (BCP) and the Resource Access Control Facility (RACF), a z/OS component that is used by different services as the central instance for identification and authentication and for access control decisions. z/OS comes with management functions that allow configuring the TOE security functions to tailor them to the customer's needs.

Some elements have been included in the TOE that do not provide security functions. These elements run in authorized mode, so they could compromise the TOE if they do not behave properly. Because these elements are essential for the operation of many customer environments, the inclusion of these elements subjects them to the process of scrutiny during the evaluation and ensures that they may be used by customers without affecting the TOE's security status.

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.

Intended Method of Use:

z/OS provides a general computing environment that allows users to gain controlled access to its resources in different ways:

- online interaction with users through Time Sharing Option Extensions (TSO/E) or z/OS UNIX System Services
- batch processing (JES2)
- services provided by started procedures or tasks
- daemons and servers of the z/OS UNIX System Services that provide similar functions as started procedures or tasks based on UNIX interfaces

These services can be accessed by users local to, or with otherwise protected access to, the computer systems.

All users of the TOE are assigned a unique user identifier (user ID). This user ID, which is used as the basis for access control decisions and for accountability, associates the user with a set of security attributes. The TOE authenticates the claimed identity of a user before allowing this user to perform any further security-relevant actions.

All TOE resources are under the control of the TOE. The TOE mediates the access of subjects to TOE-protected objects. Subjects in the TOE are called tasks. Tasks are the active entities that can act on the user's behalf. Data is stored in named objects. The TOE can associate a set of security attributes with each named resource, which include the description of the access rights to that object and (in LSPP mode) a security label.

Objects are owned by users, who are assumed to be capable of assigning discretionary access rights to their objects in accordance with the organizational security policies. Ownership of named objects can be transferred under the control of the access control policy. In LSPP mode, security labels are assigned by the TOE, either automatically upon creation of the object or by the trusted system administrator. The security attributes of users, data objects, and objects through which the information is passed are used to determine if information may flow through the system as requested by a user.

Apart from normal users, z/OS recognizes administrative users with special authorizations. These users are trusted to perform system administration and maintenance tasks, which includes configuration of the security policy enforced by the z/OS system and attributes related to it. Authorizations can be delegated to other administrative users by updating their security attributes. The TOE also recognizes the role of an auditor, who uses the auditing system provided by

z/OS to monitor the system usage according to the organizational security policies.

The TOE is intended to operate in a networked environment with other instantiations of the TOE as well as other well-behaved client systems operating within the same management domain. All of those systems need to be configured in accordance with a defined common security policy.

The primary security features of the product are:

- Identification and Authentication
- Discretionary Access Control
- in LSP mode: Mandatory Access Control and support for security labels
- Auditing
- Object Re-use
- Security Management
- Secure Communication
- 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.

A detailed description of the security functions can be found in the Security Target [7], chapter 6.2 to 6.8.

The subsystems considered in the high-level design of the TOE are the following:

- z/Architecture
- Base Control Program (BCP)
- System Management Facilities (SMF)
- Security Server (RACF)
- Systems Operations
- Communications Server (IP)
- DFSMS – System Managed Storage
- JES2
- TSO/E
- z/OS UNIX System Services
- Print Services Facility – Print Labeling Function

6 Documentation

The following documentation is provided with the product by the developer to the customer:

- Memo to Customers of z/OS V1.6 Common Criteria Configuration
- ServerPac: IYO (Installing Your Order), a custom-built installation manual shipped in printed form.
- z/OS V1R6.0 Planning for Multilevel Security and the Common Criteria (IBM Document number GA22-7509-02) shipped in printed form.
- ServerPac Using the Installation Dialog (Dialog Level 17) (IBM Document number SA22-7815-09) provided on the set of documentation CD-ROMs
- z/OS V1R6.0 Information Roadmap (IBM Document number SA22-7500-07), which contains references to other relevant documents provided on a set of documentation CD-ROMs.
- Additional documents shipped on CD-ROM:
 - z/OS V1R6 Program Directory
 - z/OS V1.6 Collection
 - PSF 3.4 CDROM Kit BOOK
 - PSF 3.4 CDROM Kit PDF
 - PSF V3R4 User's Guide
 - Overlay Generation Language/370: User's Guide and Reference
 - OGL/370 V1R1.0: Getting Started
 - OGL/370 V1R1.0: LPS
 - OGL: Command Summary and Quick Reference

To get to the evaluated configuration of z/OS a user should start with the guidance documents "Memo to Customers of z/OS V1.6 Common Criteria Configuration" and "z/OS V1R6.0 Planning for Multilevel Security and the Common Criteria (IBM Document number GA22-7509-02)".

7 IT Product Testing

Test configuration

The Security Target requires the software packages comprising the TOE to be run on an abstract machine implementing the z/Architecture machine interface as defined in the "z/Architecture Principles of Operation". The hardware platforms implementing this abstract machine are:

- IBM zSeries model z800
- IBM zSeries model z890
- IBM zSeries model z900
- IBM zSeries model z990

The TOE may be running on those machines either directly or within a logical partition provided by a certified version of PR/SM. In addition, the TOE may run on a virtual machine provided by a certified version of z/VM.

IBM has tested the platforms (hardware and combinations of hardware with PR/SM and/or z/VM) for z/OS individually for their compliance to the z/Architecture using the Systems Assurance Kernel (SAK) suite of tests. These tests ensure that every platform provides the abstract machine interface that z/OS requires.

Due to the massive amount of tests, testing was performed throughout the development of the TOE. To ensure proper testing of all security relevant behaviour of the TOE, the evaluators verified that all tests that might have been affected by any security-relevant change introduced late in the development cycle had been run on the evaluated configuration. This was also proven by re-running all independent evaluator tests in the final environment.

Depth/Coverage of Testing

The developer has done substantial functional testing of all externally visible interfaces (TSFI). Internal interfaces of the High-level design have been covered by direct and indirect testing. The evaluators repeated a subset of the developer tests and conducted additional independent tests and penetration tests.

Summary of Developer Testing Effort

Test configuration:

The sponsor/developer has performed the tests on the platforms defined above. The software was installed and configured as required in the guidance documents (refer to chapter 6).

Testing approach:

The sponsor/developer conducts extensive testing for every release of z/OS. Functional Verification Testing (FVT) and System Verification Testing (SVT) are performed by independent test teams with testers being independent from developers. A special collection of tests was compiled to explicitly deal with the security functionality as claimed in the Security Target.

Testing results:

All actual test results were consistent with the expected test results.

Summary of Evaluator Testing EffortTest configuration:

The evaluator used the same abstract machines as the developer. The configuration of the TOE was conformant to the Security Target requirements and have been set up according to the guidance documents.

Testing approach:

The evaluation facility decided to re-run a subset of the developer tests covering all security functions without striving for exhaustive testing. In addition evaluator tests were defined and executed by the evaluation facility.

Testing results:

All actual test results were consistent with the expected test results.

Evaluator penetration testing:

The evaluators have devised a set of penetration tests based on

- common sources for vulnerabilities of operating systems,
- findings of their evaluation work.

The penetration testing addressed the following security functions:

- Secure Communication
- TSF Protection

with emphasis on the TSF Protection.

The penetration testing showed no obvious vulnerabilities which are exploitable in the intended operating environment.

8 Evaluated Configuration

The Target of Evaluation **IBM z/OS Version 1, Release 6**. The TOE is software only. The following product components represent the TOE:

Software Components:

z/OS Version 1 Release 6, in the “Common Criteria Evaluated Base” version consists of the following tape sets:

- z/OS V1R6 Common Criteria Evaluated Base (IBM program number 5694-A01) with enabled features:
- CBPDO tape with additional service, including RACF APAR OA09052
- IBM Print Services Facility™ Version 3 for z/OS (PSF V3R4, program number 5655-B17)
- Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191).

Guidance Documents:

- Memo to Customers of z/OS V1.6 Common Criteria Configuration
- ServerPac: IYO (Installing Your Order), a custom-built installation manual shipped in printed form.
- z/OS V1R6.0 Planning for Multilevel Security and the Common Criteria (IBM Document number GA22-7509-02) shipped in printed form.
- ServerPac Using the Installation Dialog (Dialog Level 17) (IBM Document number SA22-7815-09) provided on the set of documentation CD-ROMs
- z/OS V1R6.0 Information Roadmap (IBM Document number SA22-7500-07), which contains references to other relevant documents provided on a set of documentation CD-ROMs.
- Additional documents shipped on CD-ROM:
 - z/OS V1R6 Program Directory
 - z/OS V1.6 Collection
 - PSF 3.4 CDROM Kit BOOK
 - PSF 3.4 CDROM Kit PDF
 - PSF V3R4 User's Guide

- Overlay Generation Language/370: User's Guide and Reference
- OGL/370 V1R1.0: Getting Started
- OGL/370 V1R1.0: LPS
- OGL: Command Summary and Quick Reference

The software elements are shipped on installation tapes (3480 compressed tapes). All guidance documents are either printed or on CD-ROMs packaged and shipped with the installation tapes.

The configuration requirements for the TOE are defined in chapter 2.3.1 of the Security Target [7]. A summary can also be found in chapter 1.5 of this report.

Constraints on the abstract machine the TOE can be run on are given in the Security Target [7], chapter 2.3.2. Chapter 1.6 of this report provides a summary of the operating platform.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE (this includes especially the methodology for flaw remediation, [5]).

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ADV_SPM.1 and ALC_FLR.1 as well as the Security Target evaluation) are summarised in the following table:

Assurance Classes and Components		Verdict
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS

Assurance Classes and Components		Verdict
Vulnerability assessment	CC Class AVA	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

The evaluation has shown that the TOE fulfils the claimed strength of function for the authentication function using passwords.

The TOE has no obvious vulnerabilities which are exploitable in the intended operating environment.

The results of the evaluation are only applicable to the product IBM z/OS Version 1, Release 6 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [7] and the chapters 2, 4, and 8 of this report). The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

None.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [7] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BDT	Bulk Data Transfer
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CAPP	Controlled Access Protection Profile
CC	Common Criteria for IT Security Evaluation
DCE	Distributed Computing Environment
EAL	Evaluation Assurance Level
LSPP	Labeled Security Protection Profile
IKE	Internet Key Exchange
IPSec	Secure Internet Protocol
IT	Information Technology
JES	Job Entry Subsystem
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RACF	Resource Access Control Facility
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 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.

14 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.
- [5] Application Notes and Interpretations of the Scheme AIS33, Version 2 – “Methodologie zur Fehlerbehebung – Flaw Remediation”, 26.07.2002
- [6] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site
- [7] Security Target BSI-DSZ-0247-2005, Version 1.15, February 2005, Security Target for IBM z/OS Version 1 Release 6, IBM Corporation
- [8] Evaluation Technical Report, Version 2.0, 04.03.2005, Evaluation Technical Report BSI-DSZ-CC-0247 (confidential document)
- [9] Labeled Security Protection Profile (LSPP), Version 1.b National Security Agency, 1999-10-08
- [10] Controlled Access Protection Profile (CAPP), Version 1.d National Security Agency, 1999-10-08

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name	
Class ACM: Configuration management	CM automation	ACM_AUT	
	CM capabilities	ACM_CAP	
	CM scope	ACM_SCP	
Class ADO: Delivery and operation	Delivery	ADO_DEL	
	Installation, generation and start-up	ADO_IGS	
Class 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	
	Class AGD: Guidance documents	Administrator guidance	AGD_ADM
		User guidance	AGD_USR
	Class ALC: Life cycle support	Development security	ALC_DVS
Flaw remediation		ALC_FLR	
Life cycle definition		ALC_LCD	
Tools and techniques		ALC_TAT	
Class ATE: Tests	Coverage	ATE_COV	
	Depth	ATE_DPT	
	Functional tests	ATE_FUN	
	Independent testing	ATE_IND	
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA	
	Misuse	AVA_MSU	
	Strength of TOE security functions	AVA_SOF	
	Vulnerability analysis	AVA_VLA	

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)**AVA_SOF** Strength of TOE security functions

„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 14.4)**AVA_VLA** Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank.