Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0286-2008

for

IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6)

from

International Business Machines (IBM) Inc.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0286-2008

IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6)

from	International Business Machines (IBM) Inc.
PP Conformance:	Labeled Security Protection Profile (LSPP), Version 1.b, 8 October 1999, and the Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999
Functionality:	PP conformant plus product specific extensions, Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_SPM.1, ALC_FLR.1

Common Criteria Arrangement

Common Criteria

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

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 29. January 2008

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 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)
- 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-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

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

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

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

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6) has undergone the certification procedure at BSI.

The evaluation of the product IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6) was conducted by atsec information security GmbH. The evaluation was completed on 14. December 2007. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

For this certification procedure the sponsor and applicant is: International Business Machines (IBM) Inc.

The product was developed by: International Business Machines (IBM) Inc.

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

4 Validity of the certification result

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

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- 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 following Certification Results contain pages B-1 to B-20.

The product IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6) 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 +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] International Business Machines (IBM) Inc.
555 Bailey Avenue
San Jose, CA 95141, 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

The Target of evaluation (TOE) is the product IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6).

The target of this evaluation (TOE) is a well-chosen combination of IBM products around DB2 UDB and z/OS (for more information see section 2.4 of the Security Target [6]), which together provide a powerful DBMS with security functions fulfilling the requirements of the Controlled Access Protection Profile (CAPP) [8] and Labelled Security Protection Profile (LSPP) [9].

In the configuration chosen for this evaluation, DB2 UDB uses the access control and security management services provided by the Resource Access Control Facility (RACF) of z/OS for discretionary access controls and to implement multilevel security controls down to the granularity of individual rows in a database.

The TOE also implements mandatory access control for both z/OS and DB2 objects. In DB2 mandatory access control is implemented by a dedicated column in each table that contains the sensitivity label of the row. This column is maintained by the TOE and can not be altered by a user unless he has the specific privilege to overwrite labels.

To operate a mainframe system which deploys the products constituting this TOE in either a CAPP or LSPP mode of operation, the products must be installed in their evaluated version and configured in a secure manner as described in the directions delivered with the media and the guides especially in the documents [10], [11] and [12].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Labeled Security Protection Profile (LSPP), Version 1.b, 8 October 1999, and the Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999 ([9] and [8]).

The TOE security assurance requirements 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 3 augmented by ADV_SPM.1 and ALC_FLR.1.

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
IA	Identification and Authentication
AC	(Discretionary and Mandatory) Access Control
CS	Communication Security in z/OS
SM	Security Management
AU	Auditing
OR	Object Reuse
SP	TOE Self-protection

Table 1: TOE Security Functions

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

The claimed TOE's strength of functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 8.2.7 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

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

This certification covers the configurations of the TOE as described in chapter 2.4 of the Security Target [6].

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 DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6)

The TOE consists of

- DB2 Universal Data Base for z/OS Version 8 (Common Criteria Evaluated EAL 3+ ServerPac and two corrective service tapes)
- z/OS Version 1 Release 6 (Common Criteria Evaluated Base ServerPac and APAR OA09723)

The following table shows the detailed scope of supply:

No	Type	Identifier	Release	Form of Delivery
DB2 Universal Data Base for z/OS Version 8 Common Criteria Evaluated EAL 3+				
DB2 UDB for z/OS Version 8 (English Base), IBM program number 5625-DB2				
2	SW	DB2 UDB for z/OS Version 8 (English Base), 5625-DB2	V8R1, tape label no. 2005351064	Tape
3	DOC	DB2 UDB for z/OS Codes	GC18-9603-02	Hardcopy
4	DOC	DB2 UDB for z/OS Installation Guide	GC18-7418-05	Hardcopy
5	DOC	DB2 UDB for z/OS Licensed Library Collection CD/ROM	LK3T-7128-05	CD-ROM
6	DOC	DB2 UDB for z/OS Licensed Program Specifications	GC18-7420-01	Hardcopy
7	DOC	DB2 UDB for z/OS Messages	GC18-9602-02	Hardcopy
8	DOC	DB2 UDB for z/OS Program Directory	GI10-8566-04	Hardcopy
DB2 Utilities Suite Version 8, IBM program number 5655-K61				
9	SW	DB2 Utilities Suite for z/OS Version 8 (IBM program number 5655-K16) US English	V8R1, tape label no. 2005351064	Tape
10	DOC	Licensed Information for DB2 Utilities Suite	GC18-9086-00	Hardcopy
11	DOC	DB2 Utilities Suite for z/OS, V8R1 Program Directory	GI10-8568-02	Hardcopy
Additional media				
12	SW	US English/Service Media 1, with additional DB2 service	tape label no. B7221159,	Tape

No	Type	Identifier	Release	Form of Delivery
13	SW	US English/Service Media 2, with additional DB2 service	tape label no. B7334259	Tape
14	DOC	DB2 UDB for z/OS Requirements for the Common Criteria with the update as published at https://www-306.ibm.com/software/data/db2/zos/v8books.html	SC18-9672-00	Hardcopy, Electronic
15	DOC	ServerPac: IYO (Installing Your Order), a custom-built installation manual shipped in printed form.	n/a	Hardcopy
16	DOC	Memo to Customers of DB2 Universal Data Base for z/OS Version 8 Common Criteria Evaluated - EAL 3+	n/a	Hardcopy
z/OS V1.6 Common Criteria Evaluated Base				
z/OS V1R6 English Base V1.6.0, IBM program number 5694-A01				
17	SW	z/OS V1R6 Common Criteria Evaluated Base (IBM program number 5694-A01) with enabled features: • Communication Server Security Level 3 • DFSMS dss • RMF • SDSF • Security Server (RACF) • z/OS Security Level 3	V1R6	Tape
18	DOC	z/OS V1R6 Program Directory	GI10-0670-05	Hardcopy
19	DOC	z/OS V1.6 Collection	SK3T-4269-13	CD-ROM
20	DOC	z/OS Hot Topics Newsletter	GA22-7501-07	Hardcopy
21	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
22	DOC	Memo to Customers of z/OS V1.6 Common Criteria Configuration	n/a	Hardcopy
23	DOC	z/OS V1.6 Planning for Multilevel Security and the Common Criteria	GA22-7509-02	Hardcopy
24	SW	CBPDO tape with additional service, including RACF APAR OA09052 / PTF UA15550	n/a	Tape
25	DOC	Installation Instructions Using SMP/E: For Single Volume Physical Media	n/a	Hardcopy
PSF V3 Base for OS/390 V3.4.0, IBM program number 5655-B17				
26	SW	IBM Print Services Facility™ Version 3 for z/OS (PSF V3R4, program number 5655-B17)	V3R4	Tape

No	Type	Identifier	Release	Form of Delivery
27	DOC	PSF 3.4 CDROM Kit BOOK	SK2T926707	CD-ROM
28	DOC	PSF 3.4 CDROM Kit PDF	SK2T932501	CD-ROM
29	DOC	PSF Customization	S544562204	Hardcopy
30	DOC	PSF for OS/390 3.4.0 LPS	G544562603	Hardcopy
31	DOC	PSF for OS/390 Program Directory	GI10027100	Hardcopy
32	DOC	PSF Tiers - IBM AFP Printer	Z125456417	Hardcopy
33	DOC	PSF Tiers - Non-IBM Printer	Z125456511	Hardcopy
34	DOC	PSF V3R4 User's Guide	S544563003	Hardcopy
OGL/370 V1.1.0, IBM program number 5688-191				
35	SW	Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191)	V1R1	Tape
36	DOC	Overlay Generation Language/370: User's Guide and Reference	S544370203	Hardcopy
37	DOC	OGL/370 V1R1.0: Getting Started	G544369100	Hardcopy
38	DOC	OGL/370 V1R1.0: LPS	G544369700	Hardcopy
39	DOC	OGL: Command Summary and Quick Reference	S544370301	Hardcopy
40	DOC	Program Directory OGL/370	GI10021201	Hardcopy
Additional Media				
41	SW	APAR OA09723/PTF UA16297 must be obtained from ShopzSeries (https://www.ibm.com/software/shopzseries).	n/a	Electronic

Table 2: Deliverables of the TOE

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:

- Identification
- Authentication
- Access Control
- Audit
- Trusted Channels

Please note that a separate informal Security Policy Model has been written to fulfill the assurance requirement ADV_SPM.1. It provides more detail on the policies implemented in the TOE. The document as part of the evalution deliverables is classified as being confidential.

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:

- Installation of the TOE (OE.INSTALL)
- Physical Protection of the TOE (OE.PHYSICAL)
- Protection of access credentials (OE.CREDEN)
- Hardware separation support (OE.HW_SEP)
- Classification of information (OE.CLASSIFICATION, for the LSPP mode of the TOE only)

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

5 Architectural Information

Architectural Overview

The Target of Evaluation (TOE) is the IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 (z/OS V1R6) operating system, including the Resource Access Control Facility (RACF).

DB2 UDB V8 is a relational database management system that operates as a subsystem of z/OS. DB2 and the utilities are implemented to utilize a set of address spaces.

Users can access DB2 locally using "attachment facilities" or remote via the Distributed Data Facility which uses the DRDA protocols defined in the document:

- Open Group Technical Standard, DRDA Version 3 Vol. 1: Distributed Relational Database Architecture and
- Open Group Technical Standard, DRDA Version 3 Vol. 3: Distributed Data Management Architecture.

Attachment facilities execute in the caller's address space and communicate with the DB2 address spaces to serve requests from the user. Attachment facilities included in the evaluated configuration include the TSO attachment facility via the DSN TSO command or the DB2 ISPF panels (which in turn use the DSN command to communicate with DB2).

Another attachment facility is the Call Attach Facility (CAF), which allows programs executing under TSO or in the z/OS batch environment to communicate with DB2.

The Resource Recovery Services Attachment Facility (RRSAF) is a newer implementation of CAF with additional capabilities. RRS is a feature of z/OS that coordinates commit processing of recoverable resources in a z/OS system.

DB2 supports use of these services for DB2 applications that use the RRS attachment facility provided with DB2. The RRS attachment can be used to access resources such as SQL tables, DL/I databases, MQSeries® messages, and recoverable VSAM files within a single transaction scope.

A requester using DRDA to connect to an application server or database server uses Distributed Data Management (DDM) as part of the underlying architecture of DRDA. DDM is the data connectivity language that is used for data interchange among like or unlike systems. This allows external users to connect to DB2 and operate on DB2 databases.

The DB2 Utilities are a set of online and standalone programs providing database diagnostic and maintenance functions for administrators. The utilities do not use the standard attachment facilities and operate with the database files directly at the tablespace level.

The TOE is one instance z/OS V1R6 with DB2 UDB V8 on an abstract machine with z/OS V1R6 exercising full control over this abstract machine.

- an IBM zSeries processor (z800, z890, z900, z990 or z9-109)
- a logical partition of an IBM zSeries processor (PR/SM)
- z/VM® on a zSeries processor or on a logical partition of PR/SM

The underlying abstract machine itself is not part of the TOE, but 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 platforms selected for the evaluation consist of IBM products, which are available when the evaluation has completed and will remain available for a substantial period afterwards.

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

User identification and authentication and parts of access control to DB2 objects are provided by the Resource Access Control Facility (RACF), a z/OS Security Server component that is used by different services as the central instance for identification and authentication and for access control decisions. z/OS V1R6 and DB2 UDB V8 come with management functions that allow configuring the TSF and tailoring 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 z/OS configuration parameters are identical in the two modes.

Intended Method of Use

The TOE provides database management system services to users. Users can use SQL statements to define databases and manage their content. Several “attach facilities” exist that can be used to submit SQL statements as well as database commands from user programs to DB2. DB2 will evaluate the user’s right to perform the requested actions before satisfying the request.

The TOE is intended for application in user areas that have physical control and monitoring. The TOE will be managed by competent individuals who are supposed to be not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

The services provided by DB2 and z/OS 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 includes 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, the TOE recognizes administrative users with special authorizations. These users are trusted to perform system administration and maintenance tasks, which include configuration of the security policy enforced by the TOE 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 the

TOE 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.

Summary of Security Features

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.

  DB2 relies on the identification and authentication performed by z/OS. When checking for the user's right to use authorities managed by DB2, the database management system uses the ID of the user verified by z/OS.

- 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 are to be shared.

  In the evaluated configuration DB2 uses RACF to check for and manage access control to DB2 objects such as databases, table spaces, tables, columns, rows, indexes, and views. DB2 internal access controls based on the GRANT and REVOKE SQL statements will not be effective in the evaluated configuration.

  DAC controls are also effective for resources managed by the z/OS operating system, such as direct access storage devices (DASDs), tape data sets, and tape volumes. In the z/OS environment, 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.

With respect to mandatory access control, DB2 uses the labels defined in the RACF profiles related to DB2 objects as well as the DB2-managed labels of rows in tables. In any case the label based access checks for mandatory access control are performed using RACF.

- Audit

  The TOE provides an auditing capability that allows generating audit records for security-critical events. The audit requirements are implemented using a mix of SMF records generated by RACF and the DB2 internal trace.

  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.

  DB2 generates additional audit records as part of the DB2 trace mechanism. Those audit records are also stored in the SMF data sets. DB2 provides a utility which allows extraction and processing of those audit records.

- 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.

  In the evaluated configuration DB2 uses the functions provided by RACF to manage user profiles as well as the profiles related to DB2 objects. Access to authorities of DB2 objects is controlled by those profiles. Labels for rows in tables are assigned when they are created using the current label of the user that creates the row. The current label of the user is maintained by RACF.

- Secure communication

  The TOE 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

  DB2 uses the protection mechanisms of z/OS with RACF to protect its address space, functions and objects from unauthorized access and manipulation.

  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 Security Functions please refer to the Security Target of the TOE.

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 Security Target requires the software packages comprising the TOE to be run on an abstract machine implementing the z/Architecture machine interface. The hardware platforms implementing this abstract machine are:

- IBM zSeries model z800
- IBM zSeries model z890
- IBM zSeries model z900
- IBM zSeries model z990
- IBM System z9-109

The TOE run 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.

For DB2, the developer’s test team decided to develop their tests as automated tests within the test harness used in other DB2 testing. In general the testers

use a set of virtual machines (called EC machines) for their testing. The evaluators used the EC systems for their independent testing as well.

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.

The developer provided a mapping between the TSF of the Security Target, the TSFI in the functional specification and the tests performed. The evaluators checked this mapping and examined the test cases, verifying that the tests covered the functions and their interfaces.

The evaluators determined that developer tests provided the required coverage: Testing covered all TSF identified in the Security Target on all interfaces identified in the functional specification.

Test depth was verified against the high-level design: Based on a mapping provided by the developer the evaluators verified that all HLD subsystems were appropriately tested.

Summary of Developer Testing Effort

Test configuration:

The sponsor/developer has performed the tests on the platforms listed above. The software was installed and configured as required in the guidance documents.

Testing approach:

The sponsor/developer conducts extensive testing for every release of DB2 and 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 Effort

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

The evaluation facility re-ran all developer testcases for DB2. For z/OS the evaluators selected 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 for DB2 and z/OS based on

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

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

8 Evaluated Configuration

The TOE subject of this report is IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6). The conditions are set by the documents [6], [10], [11] and [12].

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.

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 3 package as defined in the CC (see also part C of this report)

- The components
  ADV_SPM.1 – Informal TOE security policy model
  ALC_FLR.1 – Basic flaw remediation
  augmented for this TOE evaluation.

The evaluation has confirmed:

- for PP Conformance: Labeled Security Protection Profile (LSPP), Version 1.b, 8 October 1999, and the Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999 [9]
- for the functionality: PP conformant plus product specific extensions, Common Criteria Part 2 extended
- for the assurance: Common Criteria Part 3 conformant
  EAL 3 augmented by
  ADV_SPM.1, ALC_FLR.1
- The TOE Security Function using the password mechanism fulfills 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 rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for:

- the TOE Security Function CS (Communication Security in z/OS)

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

DRDA	Distribution Relational Database Architecture
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SMF	System Management Facility
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSO	Time Sharing Option
TSP	TOE Security Policy

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

[2] Common 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.

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

[6] Security Target BSI-DSZ-0286-2008, Version 1.3.13, 2007-12-06, DB2 UDB for z/OS Security Target, IBM Corporation (public document)

[7] Evaluation Technical Report BSI-DSZ-CC-0286, Version 1.2, 2007-12-13, atsec information security GmbH (confidential document)

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

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

[10] DB2 UDB for z/OS V8 Administration Guide, 5th Edition, February 2007, IBM Corporation

[11] z/OS Planning for Multilevel Security and the Common Criteria, 3rd Edition, December 2004, IBM Corporation

[12] Requirements for the Common Criteria (IBM Document number SC18-9672-00), IBM Corporation

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.”