Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0377-2007

for

IBM z/OS
Version 1, Release 8

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0377-2007

IBM z/OS
Version 1, Release 8

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, version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Labeled Security Protection Profile (LSPP), 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** **EAL4 augmented by ALC_FLR.3 – Systematic 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, May 16th, 2007

The President of the Federal Office
for Information Security

IT
Security
Certified

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 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

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 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 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[5]
- Common Methodology for IT Security Evaluation (CEM), 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] 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 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 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been 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) recognizes certificates issued by the national certification bodies of France and the United Kingdom within 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

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 8 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0304-2006. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0304-2006 were re-used.

The evaluation of the product IBM z/OS Version 1, Release 8 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor 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 May 16th, 2007.

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-40.

The product IBM z/OS Version 1, Release 8 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 vendor[7] 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

The Target of Evaluation (TOE) is IBM z/OS Version 1, Release 8.

z/OS is a general-purpose, multi-user, multi-tasking operating system for enterprise computing systems running on IBM zSeries or z9 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 one of the following:

- a logical partition provided by PR/SM on an IBM System z™ processor (z890, z990, z9 109, z9 BC, or z9 EC);
- a certified version of z/VM® executing directly on one of the above-listed System z™ processors or in a logical partition provided by PR/SM.

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 cooperating hosts, operating under and implementing the same set of security policies.

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 IT product IBM z/OS Version 1, Release 8 was evaluated by atsec information security GmbH. The evaluation was completed on May 9th, 2007.

The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

IBM Corporation
2455 South Road
Poughkeepsie NY 12601 - USA

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 Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: ALC_FLR.3	Life cycle support – Systematic flaw remediation

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	**Security Audit**
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

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	**Addressed issue**
FCS	**Cryptographic support**
FCS_CKM.1(1)	Cryptographic key generation (TLS/SSL: symmetric algorithms)
FCS_CKM.1(2)	Cryptographic key generation (IPSec: symmetric algorithms)
FCS_CKM.1(3)	Cryptographic key generation (SSH: symmetric algorithms)
FCS_CKM.1(4)	Cryptographic key generation (z/OS Network Authentication Service: symmetric algorithms)
FCS_CKM.1(5)	Cryptographic key generation (public/private Keys)
FCS_CKM.1(6)	Cryptographic key generation (SSH: host public/private Keys)
FCS_CKM.2(1)	Cryptographic key distribution (RSA and DSA public keys)
FCS_CKM.2(2)	Cryptographic key distribution (TLS/SSL: symmetric keys)
FCS_CKM.2(3)	Cryptographic key distribution (IPSec: Diffie-Hellman key exchange for symmetric session keys)
FCS_CKM.2(4)	Cryptographic key distribution (SSH: Diffie-Hellman key exchange for symmetric session keys)
FCS_CKM.2(5)	Cryptographic key distribution (z/OS Network Authentication Service: session keys)
FCS_COP.1(1)	Cryptographic operation (RSA and DSA signatures)
FCS_COP.1(2)	Cryptographic operation (TLS/SSL: symmetric operations)
FCS_COP.1(3)	Cryptographic operation (IPSec: payload encryption)
FCS_COP.1(4)	Cryptographic operation (IPSec: HMAC-SHA)
FCS_COP.1(5)	Cryptographic operation (SSH: symmetric operations)
FCS_COP.1(6)	Cryptographic operation (z/OS Network Authentication Service: symmetric operations)
FDP	**User data protection**
FDP_ACC.1	Discretionary access control policy
FDP_ACF.1(1)	Discretionary access control functions for non-LDAP, non-z/OS UNIX objects
FDP_ACF.1(2)	Discretionary access control functions for z/OS UNIX objects

Security Functional Requirement	**Addressed issue**
FDP_ACF.1(3)	Discretionary access control functions for LDAP LDBM objects
FDP_ETC.1 (LSPP mode only)	Export of unlabeled user data
FDP_ETC.2 (LSPP mode only)	Export of labeled user data
FDP_IFC.1 (LSPP Mode Only)	Mandatory access control policy
FDP_IFF.2 (LSPP mode only)	Mandatory access control functions
FDP_ITC.1 (LSPP mode only)	Import of unlabeled user data
FDP_ITC.2 (LSPP mode only)	Import of labeled user data
FDP_RIP.2	Object residual information protection
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA	**Identification and authentication**
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	**Security Management**
FMT_MSA.1(1)	Management of object security attributes
FMT_MSA.1(2) (LSPP mode only)	Management of object security attributes for MAC
FMT_MSA.2	Secure security attributes
FMT_MSA.3(1)	Static attribute initialization
FMT_MSA.3(2) (LSPP mode only)	Static attribute initialization for MAC
FMT_MTD.1(1)	Management of the audit trail
FMT_MTD.1(2)	Management of audited events
FMT_MTD.1(3)	Management of user attributes
FMT_MTD.1(4)	Management of authentication data
FMT_MTD.1(5)	Management of cryptographic keys
FMT_MTD.1(6)	Management of additional TOE configuration data
FMT_REV.1(1)	Revocation of user attributes
FMT_REV.1(2)	Revocation of object attributes
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security management roles

Security Functional Requirement	Addressed issue
FPT	**Protection of the TOE Security Functions**
FPT_RVM.1	Reference mediation
FPT_STM.1	Reliable time stamps
FPT_TDC.1 (LSPP mode only)	Inter-TSF basic TSF data consistency
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF trusted channel

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FDP	**User data protection**
"Note 1" as defined in LSPP/CAPP	Subject residual information protection

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
Requirements for the underlying abstract machine	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security-attribute-based access control
FMT_MSA.3	Static attribute initialization
FPT_AMT.1	Abstract machine testing
Requirements for the cryptographic features of the z/Architecture (CPACF)	
FCS_COP.1(1E)	Cryptographic operation (DES)
FCS_COP.1(2E)	Cryptographic operation (AES)
FCS_COP.1(3E)	Cryptographic operation (SHA-1)

Security Functional Requirement	**Addressed issue**
Requirements for the cryptographic features of cryptographic co-processors (PCIXCC and CEX2)	
FCS_COP.1(5E)	Cryptographic operation (RSA)
FCS_CKM.1(1E)	Cryptographic key generation (Public/Private Keys)
FCS_COP.1(6E)	Cryptographic operation (RSA)

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	**Addressed issue**
Identification and Authentication	z/OS provides identification and authentication of users by the means of: • an alphanumeric RACF user ID and a system-encrypted password. • an alphanumeric RACF user ID and a PassTicket • an x.509v3 digital certificate • a Kerberos^{TM} v5 ticket • an LDAP bind DN and a RACF password For the circumstances in which the different authentication means are used, please refer to the ST.
Discretionary Access Control	z/OS 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), DASD and tape data sets, and tape volumes that are under their control are to be shared. z/OS provides three DAC mechanisms. • The z/OS standard DAC mechanism is used for most traditional (non-UNIX) protected objects. • The z/OS UNIX DAC mechanism is used for z/OS UNIX objects (files, directories, etc.) • The z/OS LDAP LDBM DAC mechanism is used to protect LDAP objects in the LDAP LDBM backend data store.
Mandatory Access Control	In addition to DAC, z/OS provides mandatory access control (MAC) functions that are required for LSPP mode, which impose additional access restrictions on information flow 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

TOE Security Function	Addressed issue
	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 labeled information if their security labels dominate the information's label, and that they can only write to labeled information containers if the container's label dominates the subject's, thus implementing the Bell-LaPadula model of information flow control. Note that security labels can be used in CAPP mode, too, if allowed by the security administrator.
Audit	The TOE provides an auditing capability that allows generating audit records for security-critical events. RACF provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access resources. 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 Reuse	The TOE ensures the re-usability of protected objects and storage before making it accessible to further use.
Security Management	z/OS provides a set of commands and options to adequately manage the TOE's security functions. Additionally, the TOE provides the capability of managing users and groups of users via the z/OS LDAP server, which can accept LDAP-format requests from a remote administrator and transform them into RACF administrative commands via its SDBM backend processing. The TOE recognizes several authorities that are able to perform the different management tasks related to the TOE's security: • General security options are managed by security administrators. • In LSPP mode: management of MAC attributes is performed by security administrators. • Management of users and their security attributes is performed by security administrators. Management of groups (and to some extent users) can be delegated to group security administrators. • Users can change their own passwords, their default groups, and their user names (but not their user IDs). • In LSPP mode: users can choose their security labels at login, for some login methods. (Note: this also applies in CAPP mode if the administrator chooses to activate security label processing.) • Auditors manage the parameters of the audit system (a list of audited events, for example) and can analyze the

TOE Security Function	Addressed issue
	audit trail. • Security administrators can define what audit records are captured by the system. • Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators.
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, labels need not to be assigned and evaluated for any communication channel. z/OS TCP/IP provides the means for associating labels with all IP addresses in the network. In LSPP mode, communication is permitted between any two addresses that have equivalent labels. z/OS TCP/IP provides the means to define Virtual IP addresses (VIPAs) with specific labels on a multilevel system. z/OS TCP/IP considers the user's label when choosing a source address for communications. Means implemented in z/OS for securing the communication: • SSL/TLS optionally with x509-based client authentication • IPSEC with IKE key exchange method • Kerberos^{TM} version 5 networking protocols • IBM Ported Tools (SSH v2 implementation) • Access controlled TCP/IP stacks
TSF Protection	TSF protection is based on several protection mechanisms that are supported by the underlying abstract machine the TOE is executed upon.

Table 5: Security Functions

For more details please refer to the Security Target [8], chapter 2.2 and 6.

1.3 Strength of Function

The TOE’s strength of functions is claimed ‘medium’ (SOF-medium) for specific functions as indicated in the Security Target [8], chapter 1.4, 8.2.7 and 8.3.4.

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.

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 OSPs. Therefore no threats have been defined in [8].

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 [8], chapter 3.4:

Name of OSP	Summary
P.AUTHORIZED_USERS	Only those users who have been authorized to access the 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 (LSPP mode only)	The system must limit the access to information based on sensitivity, as represented by a label, of the information contained in objects, and the formal clearance of users, as represented by subjects, to access that information. The access rules enforced prevent a subject from accessing information which is of higher sensitivity than it is operating at and prevent a subject from causing information from being downgraded to a lower sensitivity.

Table 6: Organisational Security Policies (OSPs)

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in chapter 2.3 and subsequent chapters of the Security Target [8] 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.
- Installations may choose not to use any of the elements delivered within the ServerPac, but are required to install, configure, and use at least the RACF component of the z/OS Security Server element.
- In addition, any software outside the TOE may be added without affecting the security characteristics of the system, if it cannot run:
  - in supervisor state
  - as APF-authorized

  - with keys 0 through 7
  - with UID(0),
  - with authority to FACILITY resources BPX.DAEMON, BPX.SERVER, or BPX.SUPERUSER
  - with authority to UNIXPRIV resources

  This explicitly excludes replacement of any element in the ServerPac providing security functions relevant to this evaluation by other third-party products.

- The IBM Tivoli Directory Server for z/OS component (also refered to as "z/OS LDAP server" in the remainder of the report) may be used as the LDAP server, but:

  - Client authentication via digital certificates has not been evaluated for LDAP and cannot be used in the evaluated configuration.
  - Client authentication using the Kerberos mechanism has not been evaluated for LDAP and cannot be used in the evaluated configuration.
  - Authentication via passwords stored in LDAP cannot be used. Authentication must occur using RACF passwords. Note that for LDBM an LDAP bind DN is specified when binding to the server, but the password specified must be for the RACF user ID associated with that LDAP bind DN by the LDAP administrator.
  - Only the LDBM configuration may be used in LSPP mode. In CAPP mode either LDBM or SDBM may be used. Other LDAP back-end configurations have not been evaluated and may not be used.
  - (LSPP only) Each running instance of the LDAP server must run with a single, non-SYSMULTI, non-SYSNONE, security label. Multiple server instances may run at the same time, with the same or different security labels.

  Note: z/OS also ships an older LDAP Server component as part of the Integrated Security Services element of z/OS. That server is not part of this evaluation, and must not be used in the evaluated configuration.

- Each running instance of the HTTP server must run with a single, non-SYSMULTI, non-SYSNONE, security label.
- SSHD (from IBM Ported Tools for z/OS) may be used, but if used must be configured to use protocol version 2 and either 3DES or one of the AES-based encryption suites, must be configured in privilege separation mode, and must be configured to allow only password-based authentication of users. Rhost-based and public-key based user authentication may not be used in the evaluated configuration. In LSPP mode SSHD should be configured with the SYSMULTI security label.

- The Network Authentication Service (NAS) component of the Integrated Security Services component, if used, and applications exploiting it, must satisfy the following constraints:
    - The Network Authentication Service must use the SAF (RACF) registry. The NDBM registry is not a valid configuration for this evaluation.
    - Cross Realm Trust relationships with foreign Kerberos realms is allowed, but the foreign KDC must be capable of supporting the same cipher as does the z/OS KDC.
    - In order to ensure strong cryptographic protection of Kerberos tickets, DES3 should be utilized by the z/OS KDC and any KDC participating in a cross-realm trust relationship with the z/OS KDC. DES should only be used in network environments where the threat of cryptographic attacks against the tickets and Kerberos-protected sessions is deemed low enough to justify the use of these weaker encryption protocols.
    - Applications supporting Kerberos may use a combination of application specific protocols and the GSS-API functions or the equivalent native platform callable services (the SAF R_TicketServ and R_GenSec callable services) to authenticate clients, and in client-server authentication. Only the Kerberos mechanism may be used by applications that utilize GSS-API or the equivalent native platform functions. The GSS-API and R_GenSec services also enable the encryption of sensitive application messages passed via application specific protocols. These services enable the secure communication between client and server applications. The GSSAPI services include the message integrity and privacy functions that validate the authenticity and secure the communications between clients and servers.
- The Network File System (NFS) Server may be used, but only in CAPP configurations. NFS must not be used in LSPP configurations. Kerberos-based authentication must be used. The server must be configured with the SAF or SAFEXPORT option, to ensure that all file and directory access (except possibly directory mounting) has appropriate RACF security checks made.
- SSL (Secure Sockets Layer) processing, if used, must use SSLv3 protocols. SSL and TLS (Transport Layer Security), if used, must use either triple DES (168-bit keys), AES (128- or 256-bit keys), or RC4 (128-bit keys) encryption.
- Any application performing client authentication using client digital certificates over SSL or TLS must be configured to use RACF to store the keyrings that contain the application private key and the allowed Certificate Authority (CA) certificates that may be used to provide the client certificates that the application will support. The use of gskkyman for this purpose is not part of the evaluated configuration.
- Any client that is delivered with the product that executes with the user's privileges must be used with care, since the TSF can not protect those

clients from potentially hostile programs. Passwords a user enters into those client programs that those clients use to pass to the corresponding server to authenticate the user may potentially be spoofed by hostile programs running in the user's address space. This includes client programs for telnet, TN3270, ftp, r-commands, ssh, all ldap utilities and Kerberos administration utilities that require the user to enter his password. When using those client programs the user should take care that no untrusted potentially hostile program has been called during his session.

The following elements and element components cannot be used in an evaluated system, either because they violate the security policies stated in this Security Target or because they have been removed from the evaluated configuration due to time and resource constraints of the evaluation. As they are part of the base system, either they must be not configured for use or they must be deactivated (see [10], chapter 7):

- All Bulk Data Transfer (BDT) elements: BDT, BDT File-to-File, and BDT Systems Network Architecture (SNA) NJE
- Connection Manager
- 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 H0H2380) components of the Distributed File Service element
- The Enterprise Identity Mapping component of the Integrated Security Services element
- Infoprint® Server
- JES3
- The Advanced Program-to-Program Communication / Multiple Virtual Storage (APPC/MVS) component of the BCP
- Process Manager component from the UNIX System Services Element
- The z/OS LDAP Server component of the Integrated Security Services element (FMID JRSL362). For LDAP functionality in the evaluated configuration use the IBM Tivoli Directory Server for z/OS (FMID HRSL380) component of z/OS instead.
- The use of TCP/IP communication for JES2 NJE has not been part of the evaluation and cannot be used in the evaluated configuration.
- The JES2 Execution Batch Monitor (XBM) facility 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.

Note: The evaluated software configuration is not invalidated by installing and operating other appropriately certified components that possibly run authorized. However the evaluation of those components must show that the component and the security policies implemented by the component do not undermine the security policies described in this document.

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 [8], chapter 2.3.2 and are summarized here:

The TOE is running 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 z890, optionally with CryptoExpress2 card or PCIXCC and PCICA crypto cards
- IBM zSeries model z990, optionally with CryptoExpress2 card or PCIXCC and PCICA crypto cards
- IBM System z9 109, z9 BC, or z9 EC, optionally with CryptoExpress2 card.

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

The following peripherals can be used with the TOE, while still preserving the security functionality:

- All terminals that are supported by the TOE.
- Printers
  - In CAPP mode: any printer that is supported by the TOE.
  - In LSPP mode: any printer that is used to print output with different security labels must support the Guaranteed Print Labeling Function. Guaranteed print labeling works with a subset of Advanced Function Presentation™ (AFP™) printers and ensures the integrity of the identification label by preventing the user from changing the label. Review the printer hardware documentation or contact the printer vendor to determine if a printer supports this function.
- All storage and backup devices supported by the TOE, such as:
  - Direct access storage devices (DASDs), except RVA devices.
  - Tape drives.
- All Ethernet and token-ring network adapters that are supported by the TOE.

Note: the peripherals may be virtualized in the case of the TOE executing within a logical partition or z/VM. The logical partitioning software and z/VM software is part of the abstract machine and therefore part of the TOE environment.

The following constraints concerning the operating environment are made in the Security Target. They are based on the assumptions defined in [8], chapter 3.2. (Please refer to the Security Target for the precise and more detailed definition):

Name of Assumption	**Summary**
Physical Assumptions	
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
Personnel Assumptions	
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperative manner in a benign environment.
Procedural Assumptions	
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.
Connectivity Assumptions	
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE may be deployed in networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address the need to trust external systems or the communication links to such systems.
A.CONNECT	All connections to peripheral devices and other systems reside within the controlled access facilities unless they are protected by TLSv1, SSLv3, SSHv2, GSSAPI with a Kerberos

Name of Assumption	Summary
	v5 mechanism using GSSAPI message wrap and unwrap functions, or IPSec. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals or job entry stations are assumed to be adequately protected.

Table 7: Assumptions for the Operational Environment of the TOE

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 (TOE) is called:

IBM z/OS Version 1, Release 8

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
z/OS Version 1 Release 8 (V1R8) Common Criteria Evaluated Base Package (consisting of):				
1	SW	z/OS Version 1 Release 8	z/OS V1R8, program number 5694-A01	Tape
2	SW	Overlay Generation Language Version 1	OGL V1R1, program number 5688-191	Tape
3	SW	IBM Print Services Facility™ Version 4 Release 1 for z/OS	PSF V4R1, program number 5655-M32	Tape
4	SW	IBM Ported Tools for z/OS V1.1.0 (optional)	FMID HOS1110, program number 5655-M23	Tape
Patches				
5	SW	APARs OA17140 (PTF UA31073), OA18669 (PTF UA30713) and OA18717 (PTF UA30706) for NFS	n/a	Download
6	SW	APARs OA18791 (PTFs UA31038 and UA31039), and OA19286 (PTF UA32981 and UA32983) for IBM Tivoli Directory Server for z/OS	n/a	Download

No	Type	Identifier	Release	Form of Delivery
7	SW	APARs OA17870 (PTF UA30109) OA19458 (PTF UA31736) OA18305 (PTF UA31003) PK36027 (PTF UK21260)	n/a	Download
8	SW	APAR PK35609 (PTF UK20846) (required only for LSPP configurations)	n/a	Download
User Guidance Documentation				
9	DOC	z/OS Planning for Multilevel Security and the Common Criteria	GA22-7509-06	CD-ROM or shipped in printed form together with the tapes

Table 8: Deliverables of the TOE

Please note that:

- The same software elements are used in the LSPP and CAPP mode of operation, except as otherwise noted. The mode of operation is defined by the configuration of the labeling-related options in RACF. Details are described in [10].
- Only the most important CC guidance documentation is listed above. More information on guidance documents (which are also shipped together with the TOE) and which have to be followed can be found in chapter 6 of this report.

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 and FIA_SOS.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_MSA.3, FMT_REV.1, FPT_TDC.1
  - A Discretionary Access Control Policy that is defined by the SFRs FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.2, 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 [8], chapters 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)

LSPP 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 [8], chapters 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 reside within the controlled access facilities unless they are protected by TLSv1, SSLv3, SSHv2, GSSAPI with a Kerberos v5 mechanism using GSSAPI message wrap and unwrap functions, or IPSec.

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 [8].

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.

For purposes of evaluation, 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:

- a logical partition provided by PR/SM on an IBM System z™ processor (z890, z990, z9 109, z9 BC, or z9 EC).
- a certified version of z/VM® executing directly on one of the above-listed System z™ processors or in a logical partition provided by PR/SM

The abstract machine itself is not part of the TOE, rather it belongs to the TOE environment. Nevertheless, the correctness of separation and memory protection mechanisms implemented in the abstract machine is analysed as part of the evaluation since those functions are crucial for the security of the TOE.

The TOE environment, as part of the System z processor, also includes specific hardware functions that provide support for the cryptographic operations involved in communications security and for the digital signature operations involved with X.509v3 digital certificates.

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 cooperating 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 of 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 (unless otherwise mentioned in chapter 2 of this report) 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 utilizing z/OS UNIX System Services that provide similar functions as started procedures or tasks but based on UNIX interfaces.

These services can be accessed by users local to the computer systems or accessing the systems via network services supported by the evaluated configuration.

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. In most cases the TOE authenticates the claimed identity of a user before allowing this user to perform any further security-relevant actions. Exceptions to this authentication policy include:

1. Pre-specified identities:

a) The authorized administrator can specify an identity to be used by server or daemon processes or system address spaces, which may be started either automatically or via system operator commands;

b) The authorized administrator may configure a trusted HTTP server to access selected data under a specified identity, rather than the identity of the end user making the request. The HTTP server may optionally authenticate the user in this case, or may serve the data to anyone asking for it, if the administrator has determined that such anonymous access is appropriate.

2. Users are allowed to execute programs that accept network connections on ports the user has access to. In this case the untrusted program has no knowledge about the external "user" and cannot perform authentication. The program executes with the rights of the z/OS user that started it, and any data access occurs using this user’s authenticated identity.

The TOE provides mechanisms for both mandatory and discretionary access control. The Security Target describes two modes of operation: one with discretionary access control only (compliant to the requirements of the "Controlled Access Protection Profile" [6]) and one with both discretionary and mandatory access control where the mandatory access control is fully enabled for all subjects and objects (compliant to the requirements of the "Labelled Security Protection Profile" [7]). In commercial environments it is often useful to activate only part of the mandatory access control functions required in this Security Target for full compliance to LSPP. While such a mode may be useful for specific environments and the functions used have been evaluated, the claims about information flow control made in the Security Target for the LSPP mode may not hold completely when only part of the mandatory access control functions are configured.

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, 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.

Summary of Security Features

The primary security features of the product are:

- Identification and authentication
- Discretionary access control
- In LSPP mode: mandatory access control and support for security labels
- Auditing
- Object re-use
- Security management
- Communications security
- 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.

Identification and authentication

z/OS provides identification and authentication of users by the means of:

- An alphanumeric RACF user ID and a system-encrypted password.
- An alphanumeric RACF user ID and a PassTicket, which is a cryptographically-generated password substitute encompassing the user ID, the requested application name, and the current date/time.
- An x.509v3 digital certificate presented to a server application that uses System SSL or TCP/IP Application Transparent TLS (AT-TLS) to provide TLS- or SSLv3-based client authentication, and then “mapped” (using TOE functions) by that server application or by AT-TLS to a RACF user ID.
- A Kerberos v5 ticket presented to a server application that supports the Kerberos mechanism, and then mapped by that application through the TOE-provided GSS-API programming services or alternate functions that are also provided by the TOE (specifically the R_ticketServ, and R_GenSec services). These functions enable the application server to validate the

Kerberos ticket, and thus the authentication of the principal. The application server then translates (or maps) the Kerberos principal (using the TOE provided function of R_userMap) to a RACF user ID.

- An LDAP bind DN, which is mapped to a RACF user ID by information in the LDAP directory, together with a password. The LDAP server then passes the derived RACF user ID, and the password, to RACF to complete the authentication process.

In the evaluated configuration, all human users are assigned a unique user ID. This user ID supports individual accountability. The TOE security functions authenticate the claimed identity of the user by verifying the password (or other mechanism, as listed above) before allowing the user to perform any actions that require TSF mediation, other than actions that aid an authorized user in gaining access to the TOE.

In some cases of external access to the system, such as the HTTP server, or LDAP server, an installation may decide to define a user ID that is used for access checking of selected resources for users that have not been authenticated. This allows an installation to define resources unauthenticated users may access using that server via an appropriate client program. Users may still authenticate to the server using their user ID and password (or other authentication mechanism as above) to access additional resources they have been assigned access to.

The required password quality can be tailored to the installation’s policies using various parameters. When creating users, administrators are required to choose an initial password that must usually be changed by the user during initial logon.

Discretionary access control

z/OS 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), DASD and tape data sets, and tape volumes that are under their control are to be shared.

RACF makes access control decisions based on the user’s identity, security attributes, group authorities, and the access authority specified with respect to the resource profile.

z/OS provides three DAC mechanisms:

1. The z/OS standard DAC mechanism is used for most traditional (non-UNIX) protected objects.
2. The z/OS UNIX DAC mechanism is used for z/OS UNIX objects (files, directories, etc.)
3. The z/OS LDAP LDBM DAC mechanism is used to protect LDAP objects in the LDAP LDBM back-end data store.

z/OS standard DAC mechanism

Access types that can be granted are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER, which form a hierarchical set of increasing access authorities.

Access authorities to resources are stored in profiles. Discrete profiles are valid for a single, named resource and generic profiles are applicable to a group of resources, typically with similar names. For access permission checks, RACF always chooses the most specific profile for a resource. Profiles can have an access control list associated with them that contains a potentially large number of entries for different groups and users, thus allowing the modeling of complex, fine-grained access controls.

Profiles are assigned to a number of resources within z/OS. This Security Target defines the resource types analyzed during the evaluation. RACF profiles are also used to manage and control privileges in z/OS and resources of subsystems that are not part of the evaluated configuration (e. g. DB2, CICS, JES3).

Access rights for subjects to resources can be set by the profile owner and by the system administrator.

z/OS UNIX DAC mechanism

z/OS implements POSIX-conformant access control for such named objects in the UNIX realm as UNIX file system objects and UNIX inter-process communication (IPC) objects.

Access types for UNIX file system objects are read, write, and execute/search, and read and write for UNIX IPC objects. z/OS file system objects provide either access control based on the permission bits associated with a file, or based on access control lists, which are upward-compatible with the permission bits algorithm and implement the recommendations from Portable Operating System Interface for UNIX (POSIX) 1003.1e draft 17.

z/OS LDAP DAC mechanism

The z/OS LDAP server supports several back-end data stores, two of which (LDBM, SDBM) can be used in the evaluated configuration. The SDBM back-end allows RACF administration by remote administrators for systems configured in CAPP mode. The LDBM back-end allows storage of customer data in either CAPP or LSPP mode, and this back-end supports a standard LDAP access control mechanism to control which authenticated users can access which data. It also supports the possibility of “public” data, accessed by unauthenticated users, when the administrator has configured this kind of data and access.

Mandatory access control and support for security labels in LSPP mode

In addition to DAC, z/OS provides mandatory access control (MAC) functions that are required for LSPP mode, which impose additional access restrictions on information flow 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 labeled information if their security labels dominate the information's label, and that they can only write to labeled information containers if the container's label dominates the subject's, thus implementing the Bell-LaPadula model of information flow control. The system can also be configured to allow write-down for certain authorized users.

MAC checks are performed before DAC checks.

Note that security label checking will also occur in CAPP mode, if the administrator has configured security labels and if resources and users have labels assigned to them. The exact effects (e.g., whether write-down can occur) depend on several RACF options, and so the behavior may differ from that imposed by an LSPP configuration, which mandates the setting of certain options.

Users with clearance for multiple security classifications can choose their label at login time in TSO and for batch jobs submitted to JES, with appropriate defaults assigned if no labels are chosen. The choice may be restricted by the label assigned to the point of access (the logical or physical device the user has used to authenticate, e. g. the ID of the terminal, the IP address, or the ID of the job entry station).

TCP/IP applications that process user login requests must either be restricted to a single label or must restrict the user label by the label assigned to the point of access.

The z/OS LDAP server has no mechanisms in the LDBM back-end to perform MAC checking. Instead, each z/OS LDAP server must run with a single security label, matching the classification of the data in the LDBM database. TCP/IP processing will then ensure that only users running with that security label will have access to the LDAP data, thus fulfilling the required MAC checking. As needed, customers may configure multiple z/OS LDAP servers, each running with a single security label, and users must connect to the appropriate server that matches their own security label when they want to access the data.

Auditing

The TOE provides an auditing capability that allows generating audit records for security-critical events. RACF provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access resources. 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.

The system can be configured to halt on exhaustion of audit trail space to prevent audit data loss. Operators are warned when audit trail space consumption reaches a predefined threshold.

RACF always generates audit records for such events as unauthorized attempts to access the system or changes to the status of the RACF database. The security administrator, auditors, and other users with appropriate authorization can configure which additional optional security events are to be logged. In addition to writing records to the audit trail, messages can be sent to the security console to immediately alert operators of detected policy violations. RACF provides SMF records for all RACF-protected resources (either “traditional” or z/OS UNIX-based) as well as for LDAP-based resources.

Auditors can unload selected parts of the SMF database for further analysis into human-readable formats or for upload to a query or reporting package, such as DFSORT™.

Object re-use functionality

Reuse of protected objects and of storage is handled by various hardware and software controls, and by administrative practices.

All memory content of non-shared page frames is cleared before making it accessible to other address spaces or data spaces. DASD data sets can be purged during deletion with the RACF ERASE option and tape volumes can be erased on return to the scratch pool. All resources allocated to UNIX objects are cleared before reuse. Other data pools are under strict TOE control and cannot be accessed directly by normal users.

Security management

z/OS provides a set of commands and options to adequately manage the TOE’s security functions. Additionally, the TOE provides the capability of managing users and groups of users via the z/OS LDAP server, which can accept LDAP-format requests from a remote administrator and transform them into RACF administrative commands via its SDBM backend processing.

The TOE recognizes several authorities that are able to perform the different management tasks related to the TOE’s security:

- General security options are managed by security administrators.
- In LSPP mode: management of MAC attributes is performed by security administrators.
- Management of users and their security attributes is performed by security administrators. Management of groups (and to some extent users) can be delegated to group security administrators.
- Users can change their own passwords, their default groups, and their user names (but not their user IDs).

- In LSPP mode: users can choose their security labels at login, for some login methods. (Note: this also applies in CAPP mode if the administrator chooses to activate security label processing.)
- Auditors manage the parameters of the audit system (a list of audited events, for example) and can analyze the audit trail.
- Security administrators can define what audit records are captured by the system.
- Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators.

Communications Security

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, labels need not to be assigned and evaluated for any communication channel.

z/OS TCP/IP provides the means for associating labels with all IP addresses in the network. In LSPP mode, communication is permitted between any two addresses that have equivalent labels. In LSPP mode, communication between two multilevel addresses requires the explicit labeling of each packet with the sending user's label and is only permitted over XCF links within the sysplex.

z/OS TCP/IP provides the means to define Virtual IP addresses (VIPAs) with specific labels on a multilevel system. z/OS TCP/IP considers the user's label when choosing a source address for communications. z/OS UNIX Systems Services also provides the means to run up to eight instances of the z/OS TCP/IP stack which can each be restricted to a single label. Either of these approaches can be used to ensure that most communications between multilevel systems do not use a multilevel address on both ends and thereby avoid the need for explicit labelling.

In its evaluated configuration, z/OS supports trusted communication channels for TCP/IP connections. The confidentiality and integrity of network connections are assured by Secure Sockets Layer / Transport Layer Security (SSL/TLS) encrypted communication for TCP/IP connections, which can be used explicitly by applications or applied transparently to their communications without changing the applications using it (assuming the applications that do not make use of the SSL/TLS capabilities that allow clients to authenticate to the system using a client-supplied X.509 digital certificate. If applications accept client certificates then they do need to have specific SSL/TLS-related processing within the applications.).

In addition to the SSL/TLS connection, z/OS also supports the IP Security (IPSec) protocol with Internet Key Exchange (IKE) as the key exchange method. This is an additional way to set up a trusted channel to another trusted IT product for IP-based connections.

z/OS also supports Kerberos^{TM} version 5 networking protocols, via the Integrated Security Services Network Authentication Service component (z/OS Network Authentication Service). These protocols enable both the client and the server to mutually authenticate. This authentication mechanism can be utilized with the GSS-API services provided by the z/OS Network Authentication Service to provide security services to applications. These services enable encrypted communications channels between clients and servers that may reside on the same or on different systems.

z/OS also supports, via the optional add-on product IBM Ported Tools for z/OS, the SSH v2 protocol and the ssh-daemon provided services of ssh (secure shell), scp (secure copy), and sftp (secure ftp).

TCP/IP-based communication can be further controlled by the access control function for TCP/IP connections, which allows controlling of the connection establishment based on access to the TCP/IP stack in general, individual network address and individual ports on a per-application or per-user basis.

z/OS also provides a variety of network services, all of which use RACF for identification, authentication, and access control. In the evaluated configuration, terminal services are provided by TN3270, telnet, rlogin, rsh, and rexec. File transfer services are provided by the File Transfer Protocol (FTP), sftp and scp, web serving functions are provided by the z/OS HTTP Server.

TSF protection

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

- Privileged processor instructions are only available to programs running in the processor's supervisor state.
- Semi-privileged instructions are only available to programs running in an execution environment that is established and authorized by the TSF.
- While in operation, all address spaces as well as the data and tasks contained therein, are protected by the memory protection mechanisms of the underlying abstract machine

The TOE's address space management ensures that programs running in problem state cannot access protected memory or resources that belong to other address spaces.

Access to system services – through supervisor call (SVC) or program call (PC) instructions, for example – is controlled by the system, which requires that subjects who want to perform security-relevant tasks are authorized appropriately.

The hardware and firmware components that provide the abstract machine for the TOE are required to be physically protected from unauthorized access. The z/OS Base Control Program mediates all access to the TOE's hardware resources themselves, other than program-visible CPU instruction functions.

Tools are provided in the TOE environment to allow authorized administrators to check the correct operation of the underlying abstract machine.

In addition to the protection mechanism of the underlying abstract machine, the TOE also uses software mechanisms like the authorized program facility (APF) or specific privileges for programs in the UNIX system services environment to protect the TSF.

High-level Design

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

1. Base Control Program (BCP)
2. System Management Facilities (SMF)
3. Security Server (Resource Access Control Facility RACF)
4. System Operations
5. Communication Server (IP and SNA)
6. DFSMS – System Managed Storage
7. Job Entry Subsystem 2 - JES2
8. TSO/E
9. z/OS UNIX System Services
10. Print Services Facility (PSF)
11. Parallel Sysplex
12. Cryptographic Services
13. Hardware Configuration Definition (HCD) and Hardware Configuration Manager (HCM)
14. Resource Management Facility - RMF
15. SDSF
16. Network File System
17. HTTP Server
18. IBM Health Checker
19. IBM Tivoli Directory Server for z/OS (LDAP)
20. Network Authentication Service (Kerberos)
21. OpenSSH
22. Common Information Model (CIM) Server

6 Documentation

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

- Memo to Customers of z/OS V1.8 Common Criteria Evaluated Base
- ServerPac: IYO (Installing Your Order), a custom-built installation manual shipped in printed form
- z/OS V1R8.0 Planning for Multilevel Security and the Common Criteria (IBM Document number GA22-7509-06), shipped in printed form
- ServerPac Using the Installation Dialog (Dialog Level 19) (IBM Document number SA22-7815-13), provided on the set of documentation CD-ROMs
- z/OS V1R8.0 Information Roadmap (IBM Document number SA22-7500-09), which contains references to other relevant documents provided on a set of documentation CD-ROMs
- Additional documents shipped on CD-ROM:
    - z/OS V1R8 Program Directory (GI10-0670-08)
    - z/OS V1.8 Collection (SK3T-4269-17)
    - z/OS V1R8 Program Directory (GI10-0670-08)
    - z/OS Hot Topics Newsletter (GA22-7501-11)
    - PSF 4.1 CDROM Kit BOOK (SK3T-9927-00)
    - PSF 4.1 CDROM Kit PDF (SK3T-9928-00)
    - Program Directory PSF V4.1 Base (GI10-0281-00)
    - PSF Tiers-AFP/IPDS Printers (Z125-4564-18)
    - Overlay Generation Language/370: User's Guide and Reference (S544370203)
    - OGL/370 V1R1.0: Getting Started (G544369100)
    - OGL/370 V1R1.0: LPS (G544369700)
    - OGL: Command Summary and Quick Reference (S544370301)
    - Program Directory OGL/370 (GI10021201)
    - Prog Dir IBM Ported Tools for z/OS V1.1.1 (GI10-0769-00)
    - IBM Ported Tools for z/OS License Information (GA22-7986-01)

All guidance documents are either printed or on CD-ROMs packaged and shipped with the installation tapes.

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 z890, optionally with CryptoExpress2 card or PCIXCC and PCICA crypto cards
- IBM zSeries model z990, optionally with CryptoExpress2 card or PCIXCC and PCICA crypto cards
- IBM System z9 109, z9 BC, or z9 EC, optionally with CryptoExpress2 card.

The TOE may be running on those machines 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.

For the peripherals that can be used with the TOE, please refer to the Security Target or chapter 1.6 of this report.

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.

The test systems were running z/OS Version 1 Release 8 in the evaluated configuration. 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.

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

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) and the Security Target.

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.

For components providing cryptographic functions, testing was performed with and without hardware cryptographic support in order to test the correct usage of the hardware cryptographic functions, if present, and the correct implementation of the software implementation within the TOE.

Testing results:

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

Summary of Evaluator Testing Effort

Test configuration:

The evaluator used the same test environment 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 focusing on functionality newly introduced since the previous evaluation. 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 evaluator has devised penetration tests based on the developer vulnerability analysis as well as on his own independent vulnerability analysis.

The evaluator has used the information contained in the evalution evidence to derive penetration tests. This time the evaluator deliberately selected very different penetration test areas compared to the previous evaluation.

The evaluator penetration tests can be classified into the following categories:

- Network vulnerability testing
- Parameter validation tests for RACF
- Tests to compromise PKI services

The penetration testing showed no vulnerabilities which are exploitable with the attack potential assumed for EAL4 in the intended operating environment.

8 Evaluated Configuration

The Target of Evaluation is IBM z/OS Version 1, Release 8**.** The TOE is software only. The following product components represent the TOE:

Software Components:

IBM z/OS Version 1, Release 8 Common Criteria Evaluated Base Package consists of the following tape sets:

- z/OS Version 1 Release 8 (z/OS V1R8, program number 5694-A01) with enabled features:
  - Communication Server Security Level 3
  - DFSMS dss
  - RMF
  - SDSF
  - Security Server (RACF)
  - CommServer Security Level 3
  - z/OS Security Level 3
- Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191)
- IBM Print Services Facility™ Version 4 Release 1 for z/OS (PSF V4R1, program number 5655-M32)
- IBM Ported Tools for z/OS V1.1.0 (FMID HOS1110, program number 5655-M23, optional

The software elements are shipped on installation tapes (3480 compressed tapes).

In addition, the following APAR packages with additional fixes need to be obtained from http://www.software.ibm.com/ShopzSeries:

- APARs OA17140 (PTF UA31073) , OA18669 (PTF UA30713) and OA18717 (PTF UA30706) for NFS.
- APARs OA18791 (PTFs UA31038 and UA31039), and OA19286 (PTF UA32981 and UA32983) for IBM Tivoli Directory Server for z/OS.
- APAR OA17870 (PTF UA30109)
- APAR PK35609 (PTF UK20846) (required only for LSPP configurations)
- APAR OA19458 (PTF UA31736)
- APAR OA18305 (PTF UA31003)
- APAR PK36027 (PTF UK21260)

When installed, these packages result in the following component versions, comprising the evaluated configuration:

- z/OS Version 1 Release 8, consisting of the z/OS V1R8 Common Criteria Evaluated Base (program number 5694-A01), with applied fixes UA30109, UA30706, UA30713, UA31003, UA31038, UA31039, UA31073, UA31736, UA32981, UA32983, UK20846, and UK21260.
- IBM Print Services Facility™ Version 4 Release 1 for z/OS (PSF V4R1, program number 5655-M32)
- Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191 V1.1.0)
- IBM Ported Tools for z/OS V1.1.0 (program number 5655-M23, V11.1, optional)

Guidance documents:

Please refer to chapter 6 of this report for a precise listing of the guidance document relevant for the certification conformant use of the TOE.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL4 (including ASE and ALC_FLR.3).

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by ALC_FLR.3 (systematic flaw remediation) and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		Verdict
Security Target evaluation	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

Assurance classes and components		Verdict
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.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
Systematic flaw remediation	ALC_FLR.3	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.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
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 9: Verdicts for the assurance components

This is a re-certification based on BSI-DSZ-CC-0304-2006. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0304-2006 were re-used. Compared to the previous certification a lot of functionality especially in the area of communication security was subject of evaluation work.

The evaluation has shown that:

- The TOE is conformant to the PPs:
  - Labeled Security Protection Profile (LSPP), Issue 1.b, 08.10.1999 and
  - Controlled Access Protection Profile (CAPP), Issue 1.d, 08.10.1999
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- The assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ALC_FLR.3 (Systematic flaw remediation).
- The following TOE Security Functions fulfil the claimed strength of function:
  - Authentication based on RACF Passwords

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).

(i) The TOE Security Functions “RACF Passtickets”, “Authentication via Client Digital Certificates”, “Authentication via Kerberos” and “Communication Security”

(ii) For other usage of encryption and decryption within the TOE.

The results of the evaluation are only applicable to IBM z/OS Version 1, Release 8 as specified in chapter 2 of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents as listed in chapter 6 of this report contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [8] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

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 2.3, 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] Controlled Access Protection Profile (CAPP), Version 1.d, National Security Agency, 1999-10-08

[7] Labeled Security Protection Profile (LSPP), Version 1.b, National Security Agency, 1999-10-08

[8] Security Target BSI-DSZ-0377-2007, Version 3.13, 2007-04-03, Security Target for IBM z/OS Version 1 Release 8, IBM Corporation

[9] Evaluation Technical Report, BSI-DSZ-CC-0377-2007. Version 1.1, 2007-05-09, atsec information security GmbH (confidential document)

User Guidance Documentation

[10] z/OS Planning for Multilevel Security and the Common Criteria, Seventh Edition, May 2007, IBM Document Number GA22-7509-06, IBM Corporation

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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.”