Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0534-2009

for

IBM z/OS
Version 1 Release 10

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0534-2009

IBM z/OS
Version 1 Release 10

from	IBM Corporation
PP Conformance:	“Controlled Access Protection Profile” (CAPP) Version 1.d, 8 October 1999
Functionality:	PP conformant plus product specific extensions; Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

Common Criteria
Recognition
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 (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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

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

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

Bonn, 13 August 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

A Certification....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC - Certificates....7
2.2 International Recognition of CC - Certificates....8
3 Performance of Evaluation and Certification....8
4 Validity of the certification result....8
5 Publication....9
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....16
2.1 Overview of Delivery Procedure....17
2.2 Identification of the TOE by the User....17
3 Security Policy....17
4 Assumptions and Clarification of Scope....18
5 Architectural Information....18
5.1 Intended Method of Use....19
5.2 Summary of Security Features....20
6 Documentation....28
7 IT Product Testing....28
7.1 Test Configuration....28
8 Evaluated Configuration....33
9 Results of the Evaluation....37
9.1 CC specific results....37
9.2 Results of cryptographic assessment....39
10 Obligations and notes for the usage of the TOE....39
11 Security Target....39
12 Definitions....39
12.1 Acronyms....39
12.2 Glossary....40
13 Bibliography....43
C Excerpts from the Criteria....45
D Annexes....55

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

---

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

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

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

3 Performance of Evaluation and Certification

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

The product IBM z/OS Version 1 Release 10 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0459-2008. Specific results from the evaluation process BSI-DSZ-CC-0459-2008 were re-used.

The evaluation of the product IBM z/OS Version 1 Release 10 was conducted by atsec information security GmbH. The evaluation was completed on 30 June 2009. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: IBM Corporation

The product was developed by: IBM Corporation

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

4 Validity of the certification result

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

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

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

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

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

5 Publication

The product IBM z/OS Version 1 Release 10 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] IBM Corporation
2455 South Road P238
Poughkeepsie
USA

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is IBM z/OS Version 1 Release 10.

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

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile “Controlled Access Protection Profile” (CAPP) Version 1.d, 8 October 1999 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL4 augmented by ALC_FLR.3.

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

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

TOE Security Function	Addressed issue
IA	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 or password phrase. ● 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). ● an LDAP bind DN, which is mapped to a RACF user ID by information in the LDAP directory, together with a password. For the circumstances in which the different authentication means are used, please refer to the Security Target [6], chapter 6.
AC	Access control *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.

TOE Security Function	Addressed issue
	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: ● The z/OS standard DAC mechanism is used for most traditional (non-UNIX, non-LDAP) 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 back-end data store. *Mandatory Access Control* In addition to DAC, z/OS provides mandatory access control (MAC) functions that are required for Labeled Security 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. 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.
CS	Communication security z/OS provides means of secure communication between systems sharing the same security policy. In Labeled Security 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 Labeled Security mode, communication is permitted between any two addresses that have equivalent labels. In Labeled Security 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 System 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. Means implemented in z/OS for securing the communication ● SSL/TLS optionally with x509-based client authentication ● IPSEC with IKE key exchange method

TOE Security Function	Addressed issue
	• Kerberos™ version 5 networking protocols • IBM Ported Tools (SSH v2 implementation) • Access controlled TCP/IP stacks
SM	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 also provides a Java class that allows Java programs to issue commands to manage users and groups. Both the LDAP SDBM and the Java class ultimately create a RACF command and pass it to RACF using a programming interface, and then RACF runs the command using the identity associated with the SDBM session or the Java program. This behaves just the same as when a local administrator issues the command, including all the same security checking and auditing. The TOE recognises 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 Labeled Security 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 or password phrases, their default groups, and their user names (but not their user IDs). • In Labeled Security mode: users can choose their security labels at login, for some login methods. • Auditors manage the parameters of the audit system (a list of audited events, for example) and can analyse 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.
AU	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 Labeled Security mode) MAC mechanisms. This audit trail can reside directly in MVS data sets, or in an MVS log stream (which can be automatically off-loaded into MVS data sets), as configured by the administrator.
OR	Object reuse

TOE Security Function	Addressed issue
	The TOE ensures protected objects and storage being cleared before making it accessible to further use.
SP	TOE self-protection TSF protection is based on several protection mechanisms that are supported by the underlying abstract machine the TOE is executed upon.

Table 1: TOE Security Functions

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 IBM PR/SM on an IBM System z™ processor (z890, z990, z9™ 109, z9™ BC, z9™ EC, z10™ BC or z10™ EC).
- a certified version of IBM z/VM® executing on one of the above-listed System z™ processors.

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.

For more details please refer to the Security Target [6], chapter 6.1 to 6.8.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

For the configuration of the TOE covered by this certification please refer to chapter 8 of this report or the Security Target [6], chapter 1.3.3.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM z/OS Version 1 Release 10

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
z/OS Version 1 Release 10 (V1R10) Common Criteria Evaluated Base Package:				
z/OS Version 1 Release 10 (z/OS V1R10, program number 5694-A01)				
1	SW	z/OS V1R10 Common Criteria Evaluated Base (IBM program number 5694-A01)	V1R10	Tape
2	DOC	z/OS V1R10 Program Directory	GI10-0670-10	Hardcopy
3	DOC	z/OS CD Collection Kit	SK3T-4269-21	CD-ROM
4	DOC	z/OS Hot Topics Newsletter	GA22-7501-15	Hardcopy
5	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
6	DOC	Memo to Customers of z/OS V1.10 Common Criteria Evaluated Base	n/a	Hardcopy
7	DOC	z/OS V1R10.0 Planning for Multilevel Security and the Common Criteria	GA22-7509-09	Hardcopy
IBM Print Services Facility™ Version 4 Release 2 for z/OS (PSF V4.2.0, program number 5655-M32)				
8	SW	IBM Print Services Facility™ Version 4 Release 2 for z/OS (PSF V4.2.0, program number 5655-M32)	V4R2	Tape
9	DOC	PSF 4.2 CDROM Kit BOOK	SK3T-9927-02	CD-ROM
10	DOC	PSF 4.2 CDROM Kit PDF	SK3T-9928-02	CD-ROM
11	DOC	PSF Tiers-AFP/IPDS Printers	Z125-4564-18	Hardcopy
OGL/370 V1.1.0 (Program number 5688-191)				
12	SW	Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191)	V1R1	Tape
13	DOC	Overlay Generation Language/370: User's Guide and Reference	S544370203	Hardcopy
14	DOC	OGL/370 V1R1.0: Getting Started	G544369100	Hardcopy
15	DOC	OGL/370 V1R1.0: LPS	G544369700	Hardcopy
16	DOC	OGL: Command Summary and Quick Reference	S544370301	Hardcopy
17	DOC	Program Directory OGL/370	GI10021201	Hardcopy
IBM Ported Tools for z/OS V1.1.3 (5655-M23)				
18	SW	IBM Ported Tools for z/OS V1.1.3 (Program number 5655-M23, optional)	V1.1.3	Tape
19	DOC	Program Directory IBM Ported Tools for z/OS V1.1.3	GI10-0769-03	Hardcopy
20	DOC	IBM Ported Tools for z/OS License Information	GA22-7986-05	Hardcopy
21	DOC	Supplementary Toolkit License Information	GA22-7986-06	Hardcopy
Additional Media				
22	SW	PTFs: UA44228, UA44851, UA44991, UA45841, UK38941, UK39926, UK41041 obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)	n/a	Electronic

Table 2: Deliverables of the TOE

2.1 Overview of Delivery Procedure

The evaluated version of z/OS can be orderd via an IBM sales representative or via the ShopzSeries web application (http://www.ibm.com/software/shopzseries). When filing an order via (secured) internet services, IBM requires customers to have an account with a login name and password. Registration for such an account in turn requires a valid customer ID from IBM.

The delivery of the tapes, CDs and Documentation occurs in one package, which is manufactured specifically for this customer and shipped via courier services. Additional maintenance can then be downloaded by the customer via the ShopzSeries web site, following the instructions delivered with the package.

2.2 Identification of the TOE by the User

The TOE reference can be verified by the administrator during initial program load (IPL), when the system identification is displayed on the system console. The operator can also issue the the operator command “D IPL INFO”, to display the z/OS version. The string "z/OS 01.10.00:" should be displayed among other information.

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
- Access Control Policies:
  - A Mandatory Access Control Policy
  - A Discretionary Access Control Policy
- An Audit Policy
- A Trusted Channel Policy

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.INSTALL
- OE.PHYSICAL
- OE.CREDEN
- OE.HW_SEP
- OE.HW_CRYPTO
- OE.CLASSIFICATION (Labeled Security Mode only)

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

5 Architectural Information

The Target of Evaluation (TOE) is the z/OS operating system with the software components as listed in chapter 2 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 IBM PR/SM on an IBM System z™ processor (z890, z990, z9 109, z9 BC, z9 EC, z10 BC or z10 EC)
- a certified version of IBM z/VM® executing on one of the above-listed System z™ processors.

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 analyzed 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 platforms selected for the evaluation consist of IBM products that are available when the evaluation has been completed and will remain available for a substantial period of time afterwards.

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

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: CAPP-compliant and Labeled Security mode. In both modes, the same software elements are used. The

two modes have different RACF settings with respect to the use of security labels. All other configuration parameters are identical in the two modes.

5.1 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 (CAPP), Issue 1.d, 08.10.1999" [7]) and one with both discretionary and mandatory access control where the mandatory access control is fully enabled for all subjects and objects. In commercial environments it is often useful to activate only part of the mandatory access control functions required in the Security Target for the Labeled Security mode. 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 Labeled Security 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 Labeled Security 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 Labeled Security 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.

5.2 Summary of Security Features

The primary security features of the product are:

- identification and authentication
- discretionary access control
- in Labeled Security 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 or (for applications that support it) password phrase.

- 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 KerberosTM 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 LDBM bind DN (which is mapped to a RACF user ID by information in the LDAP directory) or an LDAP ICTX or SDBM bind DN (which contains a RACF user ID) together with a RACF password or password phrase. The bind processing then passes the derived RACF user ID, and the password/phrase, 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/phrase (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/phrase (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 and optionally a password phrase, that must usually be changed by the user during the initial logon that uses the password/phrase.

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.

The TOE allows access decisions by this mechanism for local applications or remote applications. For local applications the application, or the TOE, uses the RACROUTE programming interface to perform the access check. Remote applications can perform similar access checking via LDAP interfaces, if the z/OS ITDS LDAP server is appropriately configured, by first authenticating (binding) with an ICTX-style identity (DN), and then providing an extended-operation request indicating that the applications wants do perform an access check. LDAP will then invoke the ICTX extended operation processing routine which will check the application’s authority to make such a request, and then will process the request if authorized. The request specifies the resource to be checked and the RACF user ID or group name whose access should be checked.

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 as well as plug-ins. Two of the data stores (LDBM, SDBM) and one plug-in (ICTX) can be used in the evaluated configuration. The SDBM back-end allows RACF administration by remote administrators for systems configured in CAPP mode. The ICTX plug-in allows remote servers to issue authorization check or auditing requests to RACF in either CAPP or Labeled Security Mode. The LDBM back-end allows storage of customer data in either CAPP or Labeled Security 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 Labeled Security mode

In addition to DAC, z/OS provides mandatory access control (MAC) functions that are required for Labeled Security 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 a Labeled Security 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.

Specifically for the z/OS LDAP server:

- The LDBM back-end has no mechanisms to perform MAC checking. Instead, each 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.
- The SDBM back-end is prohibited in Labeled Security Mode.
- The ICTX back-end does not provide any data access functions, and thus technically does not need to provide MAC checking. However, if the administrator configures ICTX in Labeled Security Mode then TCP/IP will still control an external server's connection to LDAP based on the server's security label, and any remote authorization checking requests will use that security label as part of the decision making process.

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 Labeled Security Mode) MAC mechanisms. This audit trail can reside directly in MVS data sets, or in an MVS log stream (which can be automatically off-loaded into MVS data sets), as configured by the administrator.

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.

Remote applications can use an LDAP interface to request that RACF generate an SMF audit record, if the z/OS ITDS LDAP server is appropriately configured, by first authenticating (binding) with an ICTX-style identity (DN) and then providing a extended-operation request indicating that the applications wants do generate an audit record. LDAP will then invoke the ICTX extended operation processing routine, which will check the application’s authority to make such a request, and then will process the request if authorized. The request specifies the information to be audited.

For reporting, auditors can unload all or selected parts of the SMF data for further analysis in a human-readable formats and can then upload the data to a query or reporting package, such as DFSORT™ if desired.

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 also provides a Java class that allows Java programs to issue commands to manage users and groups. Both the LDAP SDBM and the Java class ultimately create a RACF command and pass it to RACF using a programming interface,

and then RACF runs the command using the identity associated with the SDBM session or the Java program. This behaves just the same as when a local administrator issues the command, including all the same security checking and auditing.

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 Labeled Security 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 or password phrases, their default groups, and their user names (but not their user Ids).
- In Labeled Security 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 Labeled Security 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 Labeled Security Mode, communication is permitted between any two addresses that have equivalent labels. In Labeled Security 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 (AT- TLS) 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 provides centralized policy management for IPSec policies across multiple z/OS systems in the network. It also provides centralized management for digital certificates, message signing, and message verification for IPSec across multiple z/OS systems in the network.

z/OS also supports Kerberos™ version 5 networking protocols, via the Integrated Security Services Network Authentication Service component, hereafter called 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 provides also 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 be 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. System REXX
4. Security Server (Resource Access Control Facility RACF)
5. System Operations
6. Communication Server (IP and SNA)
7. DFSMS – System Managed Storage
8. Job Entry Subsystem 2 – JES2
9. TSO/E
10. z/OS UNIX System Services
11. Print Services Facility (PSF)
12. Parallel Sysplex
13. Cryptographic Services
14. Hardware Configuration Definition (HCD) and Hardware Configuration Manager (HCM)
15. Resource Management Facility – RMF
16. SDSF
17. System SSL
18. Network File System
19. HTTP Server
20. IBM Health Checker
21. IBM Tivoli Directory Server for z/OS (LDAP)
22. Network Authentication Service (Kerberos)
23. PKI Services
24. OpenSSH
25. Common Information Model (CIM) Server

26. EIM ICTX - LDAP backend for remote authorization and remote auditing

6 Documentation

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

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

7 IT Product Testing

7.1 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" [10]. 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.
- IBM System z10 Business Class, optionally with CryptoExpress2 card.
- IBM System z10 Enterprise Class, optionally with CryptoExpress2 card.

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

For the peripherals that can be used with the TOE, please refer to the Security Target, chapter 2.3.2.

IBM has tested the platforms (hardware and combinations of hardware with IBM PR/SM and/or IBM 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 10 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.

Developer Testing

An overview of IBM’s test approach, the efforts and choice of test configurations has already been provided in considerable detail in the introduction to this chapter. This section therefore provides only a brief summary of the information provided there:

- IBM tests the platforms 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 to be run. SAK testing is important not only to the z/OS evaluation, but to other evaluations (PR/SM, z/VM) as well.
- FVT for z/OS is largely performed on the VICOM test system. This is an enhanced z/VM system implementing the z/Architecture abstract machine interface. It allows testers to bring up individual, virtual test machines running z/OS with access to virtualized peripherals such as disks and network connections. For the purpose of the security function tests, this environment is fully equivalent to the machines running z/OS. This environment was also used by the evaluators for their independent testing
- Since V1R7, IBM has provided a common test framework for tests that can be automated. COMSEC is an environment that can be operated in CAPP or Labeled Security mode. The BERD (Background Environment Random Driver) test driver submits the testcases as JES2 jobs. IBM's intention is to move more and more tests to this automated environment, which will ease the test effort required for the evaluations substantially. With V1R9, and continued in V1R10, a substantial number of tests has been ported to this environment. Additionally, most test teams ran their manual tests in the COMSEC test environment, which provides a complete test environment in the evaluated configuration of the TOE in the different modes of operation.
- The test systems were running z/OS version 1 release 10 in the evaluated configuration. The SDF team provided a preinstalled system image for VICOM and for the machines running the COMSEC tests, thus ensuring that the CCEB software version was used for all tests. The additional PTFs were applied to the VICOM and COMSEC systems as they became available, with any security-relevant tests for the PTFs being sucessfully re-run.

Test approach

- IBM's general test approach is defined in the process for Integrated Product Development (IPD) with developer tests, functional verification tests (FVT), and system verification tests (SVT). Per release, an overall effort of more than 100 person years is spent on FVT and SVT for the z/OS components. FVT and SVT is performed by independent test teams, with testers being independent from the developers. The different test teams have developed their own individual test and test documentation tools, but all implement the requirements set forth in the IPD documentation.
- For the purpose of the evaluation, FVT is of interest to the evaluators, since the single security functions claimed in the [6] are tested here. IBM decided to create a test bucket with the tests for the security functions, summarizing the tests in individual test plans, so that the evaluators had a chance to deal with the otherwise overwhelming complexity of the z/OS testing.
- IBM's test strategy for the evaluation had three cornerstones:
  - The major internal security interface was the interface to RACF, which is tested exhaustively by the RACF test group
  - Components requiring Identification and Authentication or Access Control services call RACF (with the exception of LDAP LDBM, which implements its own access control). For most of these services, it is sufficient to demonstrate that these

interfaces call RACF, once the testing of the RACF interface (see above) has established confidence in the correct inner workings of RACF

- Due to the design of z/OS, a large number of internal interfaces is also visible externally, although the interfaces are not intended to be called by external, unprivileged subjects. For these interfaces, which are basically authorized programs, operator commands, certain callable services, SVC and PC routines, testing established only that these interfaces cannot be called by unauthorized callers.

Apart from these tests, all components providing external interfaces for security functions were tested intensively. For the current version of z/OS this included the newly added components for System Logger audit services, Network Security Services, Network Policy Agent, RACF handling of digital certificates (RACDCERT) for certificates stored in RACF key rings or PKCS#11 tokens, Web Express Logon services, remote authorization and auditing via the LDAP EIM ICTX backend and anonymous FTP.

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.

Test results

- The test results provided by the sponsor were generated on the configurations as described above. Although different test teams used different tools and test tracking databases, the evaluators verified that all provided results showed that tests had executed successfully and yielded the expected results.
- The testing provided was valid for both CAPP and Labeled Security modes of operation, with the exception of tests for multilevel security features, which were relevant to Labeled Security mode only. The test systems configured for Labeled Security mode are CAPP-compliant as well, so that tests run on these systems were always applicable to both modes of operation. For COMSEC, all applicable tests were run in dedicated Labeled Security and CAPP configurations.

Test coverage

The developer provided a mapping between the TSF of the [6], the TSFI in the functional specification and the tests performed. The evaluator checked this mapping and examined the test cases to verify whether the tests covered the functions and their interfaces. Although exhaustive testing is not required, the sponsor provided evidence that significant detail of the security functions have been tested.

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

Test depth

Test depth was verified against the TOE subsystems and the security enforcing modules: For most security functions relevant to this evaluation, subsystems invoke RACF functions to take security-relevant decisions; access control, identification and authentication, security management and the generation of security-relevant audit records are mostly handled by RACF. All other security-relevant functions are implemented within the subsystems themselves, thus keeping security functions isolated within them. For cryptographic functions, hardware support provided by the TOE's IT environment is

accessed through the ICSF component. Several components (like PKI Services) use the System SSL component as an intermediate provider of cryptographic functions. System SSL then checks and uses hardware support through ICSF. For the self-protection, BCP and the underlying abstract machine work together to provide memory protection and different authorization mechanisms such as APF or AKM.

The evaluators verified that all security-relevant detail of the high-level design had been taken into account for testing. In particular, testing of the RACF subsystem interfaces was performed directly at these interfaces as well as over the subsystems invoking RACF.

Conclusion

The evaluators verified that testing was performed on configurations conformant to the ST.

The evaluators were able to follow and fully understand the test approach based on the information provided by the developer.

With this test environment, the developer was able to provide proof of the necessary coverage and test depth to the evaluators. In fact, IBM provided only a small part of their overall testing to the evaluators, to help them manage the complexity of the evaluation. The evaluators were convinced by their experience in working closely with the testers during an extended period of time that the overall test coverage and test depth of IBM's testing of the security functions was even larger than the part shown to the evaluators.

Evaluator Testing Effort

The independent evaluator testing followed the CEM guidance to test every security function, without striving for exhaustive testing. For their own tests, the evaluators decided to focus on the most important security functions of the TOE in order to provide independent verification of their correct operation:

- Identification and authentication: The evaluators would only devise some basic, mostly manual testing of the Identification and authentication functions in TSO/E, telnet/rlogin, ftp, su and JES, since these functions would be exercised during the test activity implicitly by the testers. The testers also used mixed-case passwords themselves to ensure that this new feature works as specified.
- Discretionary access control: The evaluators focused on UNIX System Services ACLs, which also implicitly test UNIX permission bits. Other DAC tests involved
- USS IPC (all system calls for messages, semaphores and shared memory)
- DAC for different USS objects (device special files, IPC objects, directories)
- z/OS dataset access
- security- relevant USS system calls
- Mandatory Access Control: The evaluators re-ran their own tests on mandatory access control checks for data sets and Unix System Services files as their own regression tests. Testing of the writedown override capability provided by FACILTY class profiles was also performed.
- Communication security:The evaluators chose to ensure that secure communications channels (IPSEC and SSL) did not contain hidden platform specific implementation errors by testing interoperability with non-zSeries systems. Application-transparent TLS (AT-TLS) was also tested to work with a non-zOS platform, checking different policy settings.

- Audit: The evaluators did not develop special tests for auditing, but decided to run most of their tests with full auditing enabled and then analyze the audit records for the expected audit event records. By generating audit records in this manner a more accurate analysis the types and contents of audit records produced by the system and there contents during typical operations could be done. Dedicated tests were used to check auditing of changes to the system clock.
- Security Management:The evaluators decided to devise no special tests here, since the setup of the test environment and the setup/cleanup of the tests would already include a major portion of the TSF found here.
- TOE Self Protection: The only function to be suitably testable is object re-use, where the evaluators decided to focus on the issue of memory pages probably containing left-over information. All other self-protection features are properties that could not be easily be “challenged” by evaluator tests.

For the set of developer tests to be re-run, the evaluators chose an approach supplementing their own tests and focussing on functionality changed since the previous evaluation.

The evaluators decided to focus on security functions claimed in the Security Target and not to run tests demonstrating that functions requiring authorization would fail when invoked unprivileged. This was in part due to the fact that the evaluators had experienced already sufficient issues with protection of security functions while bringing up the system in its evaluated configuration, following the guidance in [9].

Apart from the tests re-run by the evaluators or during dedicated sessions set up for the evaluators to observe the testers running those tests, the evaluators gained confidence in the developers’ test efforts during their extended stay at the developer site, where they discussed with testers issues of testing or interpretations of the CC requirements, and were witnessing test executions while the test bucket was being created. The evaluators had already interviewed testers during the site visits and examined the test databases with test cases and test results and test execution records.

All tests were run on the VICOM test system that had been set up by the evaluators according to the specifications found in the guidance [9], and on the COMSEC system set up by IBM and verified by the evaluators to be in the evaluated configuration.

During their testing, the evaluators could verify that the test functions behaved as expected.

Evaluator Penetration Testing

Since this evaluation was a re-evaluation of a product where several previous versions had been evaluated before, and since the changes made were mainly to internals, the evaluator decided this time to focus the penetration tests on system call interfaces that are designed to be used only by IBM internal programs and where the interfaces were not or not completely described in the public documentation. The evaluator developed a framework that allows him to test system call interfaces in a controlled way by providing input “control cards” that define the interface to be tested, define the values to be placed into register (either as direct values or as address names) and define the values of storage at address names. This allows to test a system call interface by just defining the control cards that are read by the program implementing the framework. The framework program will then read those cards, initialize the storage areas and register as defined by the cards and call the system call interface. Before the interface is called the program dumps the

content of the general register and address space register as well as the system state to the output file. The program also establishes an error recovery routine that gets control if the system call detects an error (which is the expected effect for most of the tests, since the system call was called in all the tests with an invalid parameter list).

When the program returns from the system call (either to the calling program or to the error recovery routine), the content of the register and the system state is dumped again to the output file. This allows the evaluator to check if a critical value has changed unexpectedly that indicates a potential vulnerability.

The evaluator performed several tests for several system calls he has selected with different parameter values. None of the tests performed resulted in a direct privilege escalation and none of the tests showed an unexpected result that could be an indicator for a potential vulnerability.

8 Evaluated Configuration

The Target of Evaluation is IBM z/OS, Version 1 Release 10. The TOE is software only. The items listed in table TOE deliverables of this report represent the TOE.

This following configuration of the TOE is covered by this certification:

The z/OS V1R10 Common Criteria Evaluated Base package, and (if used) IBM Ported Tools for z/OS) must be installed according to the directions delivered with the media and configured according to the instructions in [9].

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;
- installing system exits that run authorized (supervisor state, system key, or APF-authorized), with the exception of the sample ICHPWX11 and its associated IRRPHREX routine;
- installing IBM Tivoli Directory Server plug-ins that have not been evaluated;
- using the Authorized Caller Table (ICHAUTAB) in RACF to allow unauthorized programs to issue RACROUTE REQUEST=VERIFY (RACINIT) or RACROUTE REQUEST=LIST (RACLIST).

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.*

The IBM Tivoli Directory Server for z/OS (FMID HRSL380) component may be used as the LDAP server, but:

- For client authentication via digital certificates the administrator must configure the LDAP server to map the certificate to a RACF user ID and to fail the bind if the certificate does not map to a RACF user ID. The allowable LDAP configuration provides three options for forming an LDBM subject:
  - LDAP may use the original DN from the certificate; or
  - LDAP may replace the original DN with an SDBM-format DN based on the RACF user ID; or
  - LDAP may add the SDBM-format DN to the LDAP subject, giving a subject with two DNs, either of which will work in LDAP ACLs.
- 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 or password phrases. Note that if an LDBM bind DN is specified when binding to the server, the password/phrase specified must be for the RACF user ID associated with that bind DN by the LDAP administrator.
- Only the LDBM back-end and the ICTX plug-in may be used in Labeled Security Mode. In CAPP mode the LDBM and SDBM back-ends and the ICTX plug-in may be used. Other LDAP back-end configurations and plug-ins have not been evaluated and must not be used.
- (Labeled Security Mode 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. However, for convenience, subsequent sections of this ST may refer to the IBM Tivoli Directory Server as the z/OS LDAP server, and to data managed by the server as "LDAP objects". In all cases, the reader should assume that references to z/OS LDAP or data managed by LDAP really indicate the IBM Tivoli Directory Server for z/OS and data managed by that server.*

Each running instance of the HTTP server must run with a security label that is neither SYSMULTI nor SYSNONE.

SSHD (from IBM Ported Tools for z/OS), may be used, but if used:

- must be configured to use protocol version 2 and either Triple DES or one of the AES-based encryption suites,
- must be configured in privilege separation mode, and
- must be configured to allow only password-based (including password phrase) authentication of users. Rhost-based and public-key based user authentication may not

be used in the evaluated configuration. In Labeled Security Mode SSHD should be configured with the SYSMULTI security label.

The Network Authentication Service 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, Triple DES or AES 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 if configured to use Kerberos-based authentication. 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 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 profiles in the RACDCERT or DIGTRING classes or PKCS#11 tokens in ICSF 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/phrases 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/phrase. 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, as described in Chapter 7, “The evaluated configuration for the Common Criteria” in z/OS Planning for Multilevel Security and the Common Criteria:

- 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 H0H2390) 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 JRSL38A). 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 must not be used in the evaluated configuration.

The JES2 Execution Batch Monitor (XBM) facility has not been part of the evaluation and must not be used in the evaluated configuration.

The RACF Remote Sharing Facility has not been part of the evaluation and must not be used in the evaluated configuration.

The Data Facility Storage Management Subsystem (DFSMS) Object Access Method for content management type applications must not be used.

For the Communications Server:

- The z/OS FTP server and client, and the z/OS TN3270 server, support both manually-configured SSL/TLS, or AT-TLS. This evaluation has considered only AT-TLS configurations, and as a result manual configuration of those components to use SSL or TLS is not allowed for evaluated configurations.
- The z/OS FTP server and client can support either the protocols from the draft standard for securing FTP with TLS/SSL, or the protocols from the formal RFC 4217 level of Security FTP with TLS/SSL. This evaluation has considered only the formal

RFC 4217 level of support, and as a result that option must be used in the evaluated configuration.

- The following applications must not be used in Labeled Security configurations, as noted in the Communications Server IP Configuration Guide: BINL, DHCP PXE, HOMETEST command, IUCV, LPD, LPQ command, LPR command, LPRM command, LPRSET command, NCPROUTE, NPF, Portmapper, SMTP, SNMP NetView client, TELNET client command, TESTSITE command, TNF, VMCF, z/OS UNIX DNS name server (BIND 4), z/OS UNIX Network SLAPM2 subagent, z/OS UNIX OMPROUTE SNMP subagent, z/OS UNIX popper, z/OS UNIX RSVP agent, z/OS UNIX SNMP client command, z/OS UNIX SNMP server and agent, z/OS UNIX Trap Forwarder Daemon.

9 Results of the Evaluation

9.1 CC specific results

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

The evaluation methodology CEM [2] was used for all assurance requirements claimed for the TOE.

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

- All components of the EAL4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0459-2008, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the transition from CC Version 2.3 to CC Version 3.1 and on the following changes relevant to security, which have been introduced in the evaluated configuration of z/OS since the previous evaluation:

- In addition to passwords, PassTickets, Kerberos tickets and digital certificates, password phrases have been introduced as a new authentication mechanism. Password phrases must be at least 9 and can be up to 100 characters long. They do not replace the password mechanism, but are an additional mechanism. This means that a user can have both a password and a password phrase, unless the administrator configures the user's account so that passwords cannot be used (e.g. by re-setting the user's password to a random string) RACF supplies additional REXX exit functions ICHPWX11 and IRRPHREX which can be used enforce some quality requirements for password phrases
- Password/phrase management has been augmented with a finer granularity. In addition to the facility class profile IRR.PASSWORD.RESET, which allows users with access to this profile to reset passwords for all normal users (except those with PROTECTED, SPECIAL, AUDITOR, or OPERATIONS attributes), additional profiles IRR.PWRESET.OWNER.owner-value and IRR.PWRESET.EXCLUDE.userID have been introduced to allow tuning of password reset rights to the granularity of single user IDs.

- Several services now also allow digital certificates as an authentication mechanism:
  - The LDAP LDBM and SDBM backends will accept digital certificates supplied over an SSL connection. LDAP uses RACF to map the certificate to a RACF user ID; If the mapping fails, LDAP will not perform the requested bind operation.
  - The FTP server accepts digital certificates.
- The management of IP filtering and Defensive filtering is handled similar to IPSEC: users allowed to add and remove dynamic or static filter rules must have access to appropriate RACF profiles in the SERVAUTH class.
- The TSO/ISPF Client Gateway is an interface users can use to invoke TSO and ISPF commands and applications. This z/OS UNIX based gateway allows client applications to use Web-based communication services such as HTTP to invoke TSO and ISPF commands. The interface is designed to provide support for multiple TSO and ISPF sessions and allows these sessions to maintain state between command invocations.
- The new System z10 entry model "IBM System z10 Business Class" has been added to the existing "IBM System z10 Enterprise Class" as a System z system suitable to run the TOE. This new z10 model can also be equipped with an optional CryptoExpress2 card, which is identical to the z10 Enterprise Class model.

The evaluation has confirmed:

- PP Conformance: “Controlled Access Protection Profile” (CAPP) Version 1.d, 8 October 1999 [1]
- for the Functionality: PP conformant plus product specific extensions; Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

For specific evaluation results regarding the development and production environment see annex B in part D of this report. The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for:

- The TOE Security Functions “RACF Passtickets”, “Authentication via Client Digital Certificates”, “Authentication via Kerberos” and “Communication Security” and
- for other usage of encryption and decryption within the TOE.

10 Obligations and notes for the usage of the TOE

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

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

ACEE	Accessor Environment Element
AT-TLS	Application-Transparent TLS
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CN	common name
DAC	Discretionary access control
DN	distinguished name
EAL	Evaluation Assurance Level
IOCDS	input/output configuration data set
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory access control
PADS	program access to data sets
PKI	Public Key Infrastructure
PP	Protection Profile
PR/SM™	Processor Resource/Systems Manager™
RACF	Resource Access Control Facility
SAR	Security Assurance Requirement
SDSF	System Display and Search Facility
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMF	System Management Facility
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE security policy

12.2 Glossary

Abstract Machine - A processor design that is not intended to be implemented as hardware, but which is the notional executor of a particular intermediate language (abstract machine language) used in a compiler or interpreter. An abstract machine has an instruction set, a register set, and a model of memory. It may provide instructions that are closer to the language being compiled than any physical computer or it may be used to make the language implementation easier to port to other platforms.

Access - If an authorized user is granted a request to operate on an object, the user is said to have access to that object. There are numerous types of access. Examples include read access, which allows the reading of objects, and write access, which allows the writing of objects.

Access Control Policy - A set of rules used to mediate user access to TOE-protected objects. Access control policies consist of two types of rules: access rules, which apply to the behavior of authorized users, and authorization rules, which apply to the behavior of authorized administrators.

Accessor Environment Element - A RACF control block that describes the current user's security environment.

Augmentation - The addition of one or more requirement(s) to a package.

Authorization - If an authorized user is granted a requested service, the user is said to have authorization to the requested service or object. There are numerous possible authorizations. Typical authorizations include auditor authorization, which allows an administrator to view audit records and execute audit tools, and DAC override authorization, which allows an administrator to override object access controls to administer the system.

Authorized Administrator - An authorized user who has been granted the authority to manage all or a defined subset of the functions of the TOE. Authorized administrators are expected to use this authority only in the manner prescribed by the guidance that is given to them.

Authorized User - A user who has been properly identified and authenticated. Authorized users are considered to be legitimate users of the TOE. (Note: this is different from the z/OS concept of an "authorized program" which is a program running in supervisor state, or system key, or with APF authority.)

Category - See security category.

Classification (MLS) - A hierarchical designation for data that represents the sensitivity of the information. The equivalent IBM term is security level.

Common Name (CN) - One component of an LDAP object's complete name, usually specified as cn=name.

Discretionary Access Control (DAC) - An access control policy that allows authorized users and authorized administrators to control access to objects based on individual user identity or membership in a group (PROJECTA, for example).

Distinguished Name (DN) - The complete name of an object in an LDAP directory, or the complete name of the subject or issuer of a digital certificate.

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.

Lightweight Directory Access Protocol (LDAP) - A client/server protocol for accessing a directory service.

Mandatory Access Control (MAC) - An access control policy that determines access based on the sensitivity (SECRET, for example) and category (PERSONNEL or MEDICAL, for example) of the information that is being accessed and the clearance of the user who is trying to gain access to that information.

Mediation - When DAC and MAC policy rules are invoked, the TOE is said to be mediating access to TOEprotected objects.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Password - For the purposes of this evaluation, a 6 to 8 character secret value used during some forms of user authentication, and allowing upper- and lower-case alphabetic, numeric, or national ($, #, @) characters. Passwords are initially assigned by administrators, but may be changed by the user to whom they are assigned.

Password Phrase - A 14 to 100 character secret value used in a manner similar to a password, except for its length and an expanded set of valid characters (upper- and lower-case alphabetic, special (including blanks), or numeric). In addition to assigning a password, administrators may assign a password phrase to a user.

Note: Phrase may be shorter (down to 9 characters) if enabled by an administrator-installed exit (ICHPWX11) that RACF supplies.

Password/Phrase - A shorthand term for “password or password phrase” sometimes used in this security target when statements apply equally to passwords or to password phrases.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

SECLABEL - Synonym for security label.

SECLEVEL - Synonym for security level (IBM).

Security Category - A special designation for data at a certain level, which indicates that only people who have been properly briefed and cleared for access to data with this category can receive permission for access to the information.

Security Label - A name that represents the combination of a hierarchical level of classification (IBM security level) and a set of non-hierarchical categories (security category). Security labels are used as the base for mandatory access control decisions. Security labels are sometimes referred to as SECLABELs.

Security Level (IBM) - A hierarchical designation for data that represents the sensitivity of the information. Security levels are sometimes referred to as SECLEVELs. The equivalent MLS term is classification.

Security Level (MLS policy in the Bell-LaPadula model) - The combination of a hierarchical classification (called security level in z/OS) and a set of nonhierarchical

categories that represents the sensitivity of information is known as the security level. The equivalent term in other IBM documentation is security label.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Sensitivity Label - A specific marking attached to subjects or objects that indicates the security level. The equivalent to this MLS term in other IBM documentation is security label.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

User - A person who is trying to invoke a service that is offered by the TOE.

User ID - In z/OS, a string of up to eight characters defined as a RACF USER profile that uniquely identifies a user. Users who may use UNIX services will additionally have a numerical user identifier (UID) that is used by the UNIX subsystem for access decisions. The user name is an additional attribute that usually holds the user's full name. While users can modify their user names, only administrators can change user IDs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

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

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

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

[6] Security Target BSI-DSZ-CC-0534, Version 5.11, 16.03.2009, Security Target for IBM z/OS Version 1 Release 10, IBM Corporation

[7] Controlled Access Protection Profile (CAPP), Issue 1.d, 08.10.1999

[8] Evaluation Technical Report BSI-DSZ-CC-0534, Version 3, 30.06.09, atsec information security GmbH (confidential document)

[9] MLSGUIDE z/OS Planning for Multilevel Security and the Common Criteria, Version GA22-7509-08, April 2009, File name agd/e0z2e150.pdf

[10] z/Architecture Principles of Operation, Version SA22-7832-07, February 2009, http://publibz.boulder.ibm.com/epubs/pdf/dz9zr007.pdf

[8] specifically

- AIS 1, Version 13, 14. August 2008, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 4, 02. April 2007, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 19, Version 4, 13. March 2009, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 23, Version 2, 11. March 2009, Zusammentragen von Nachweisen der Entwickler
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decompositon.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“ 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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0534-2009

Evaluation results regarding development and production environment

The IT product IBM z/OS Version 1 Release 10 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 4 sowie Anwendungshinweise und Interpretationen spezifisch für die Technologie des Produktes for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 13. August 2009, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

All development sites also perform testing for their components of the product. The TOE is developed and tested at the following sites:

Site	Address
Poughkeepsie (POK)	2455 South Rd, Poughkeepsie, NY 12601, USA
Research Triangle Park (RTP)	Building 500, 4205 South Miami Blvd, Durham, NC
Silicon Valley Labs (SVL)	555 Bailey Avenue, San Jose, CA 95141, USA
Boeblingen (BOE)	Schönaicher Straße 220, 71032 Böblingen, Germany
Boulder (BLD)	6300 Diagonal Highway, Boulder, CO 80301, USA
Tucson (TUC)	9000 S Rita Rd, Tucson, AZ 85744, USA
Perth (PTH)	1060 Hay St, West Perth WA 6005, Australia
Hursley (HUR)	Hursley House, Hursley Park, Winchester, Hants SO21 2JN, United Kingdom
Toronto (TOR)	8200 Warden Avenue, L6G 1C7 Markham, Ontario, Canada

Production of the media and delivery to the customer is performed at the IBM site in Boulder, CO, USA.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.