Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0972-2015

for

## z/OS Version 2 Release 1

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-0972-2015** (*)

Operating System

**z/OS**
Version 2 Release 1

from IBM Corporation

| | |
|---|---|
| PP Conformance: | General-Purpose Operating System Protection Profile Version 3.9, 6 December 2012, OSPP Technical Community |
| Functionality: | PP conformant<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant |

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4.

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.

Common Criteria
Recognition Arrangement

Bonn, 14 September 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

**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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

# Contents

# A. Certification

## 1. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- 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 (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

"Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. This Domain is linked to a conformance claim to one of the related SOGIS Recommended Protection Profiles. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

### 2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: 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 by the nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

## 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 z/OS, Version 2 Release 1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0874-2014. Specific results from the evaluation process BSI-DSZ-CC-0874-2014 were re-used.

The evaluation of the product z/OS, Version 2 Release 1 was conducted by atsec information security GmbH. The evaluation was completed on 29 July 2015. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: IBM Corporation.

The product was developed by: IBM Corporation.

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

# 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, as 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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 14 September 2015 is valid until 10 August 2020. The validity date can be extended by re-assessment or re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report and the Security Target and user guidance documentation mentioned herein to any applicant of the product for the application and usage of the certified product,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the product's evaluated life cycle, e.g. related to development and production sites or processes, occur or the confidentiality of documentation and information related to the product or resulting from the evaluation and certification procedure is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the product or resulting from the evaluation and certification procedure that do not belong to the product deliverables according to the Certification Report part B chapter 2 to third parties, permission of the Certification Body at BSI has to be obtained.

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 z/OS, Version 2 Release 1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] IBM Corporation
2455 South Road P328
Poughkeepsie NY 12601
USA

# B. Certification Results

The following results represent a summary of

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

# 1. Executive Summary

The Target of evaluation (TOE) is IBM z/OS, Version 2 Release 1.

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 evaluation. It is conformant to the Protection Profile "General-Purpose Operating System Protection Profile (GPOSPP)" [7].

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria ([CC]). ~~z/OS meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.~~

The Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], section 7.1. They are selected from Common Criteria Part 2 and from GPOSPP [7] where some SFRs have been defined as extended components. Thus z/OS is CC part 2 extended.

There also are requirements relevant for the operational environment of the TOE which are outlined following an SFR-like notation in the Security Target ([6], chapter 6).

z/OS can be configured to two modes of operation, a standard mode and a Labeled Security Mode.

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

| TOE Security Functionality | Addressed issue |
|---|---|
| Identification and Authentication | z/OS provides identification and authentication of users by the means of<br>• an alphanumeric RACF user ID and a system-encrypted password or (for applications that support it) password phrase.<br>• 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.<br>• 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-based client authentication, and then “mapped” (using TOE functions) by that server application or by AT-TLS to a RACF user ID.<br>• a Kerberos™ v5 ticket presented to a server application that supports the Kerberos mechanism, and then mapped by that application through the TOE-provided GSS-API programming services or alternate functions that are also provided by the TOE (specifically the R_ticketServ, and R_GenSec services). These functions enable the application server to validate the Kerberos ticket, and thus the authentication of the principal. The application server then translates (or maps) the Kerberos principal (using the TOE provided function of R_userMap) to a RACF user ID.<br>• 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. |

| TOE Security Functionality | Addressed issue |
|---|---|
| | • a digital certificate presented to LDAP over TLS (LDAP SASL bind with EXTERNAL verification) which must map to a RACF USER ID. |
| 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 (DASD), DASD and tape data sets, and tape volumes that are under their control are to be shared.<br>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.<br>z/OS provides the following DAC mechanisms:<br>1. The z/OS standard DAC mechanism is used for most traditional (non-UNIX) protected objects.<br>2. The z/OS UNIX DAC mechanism is used for z/OS UNIX objects (files, directories, etc.) except IPC objects<br>3. The z/OS UNIX IPC DAC mechanism is used for z/OS UNIX IPC objects (shared memory segments, semaphores)<br>4. The z/OS LDAP LDBM DAC mechanism is used to protect LDAP objects in the LDAP LDBM back-end data store. |
| 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 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. |
| Object Reuse | Reuse of protected objects and of storage is handled by various hardware and software controls, and by administrative practices.<br>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, groups of users, general resource profiles, and RACF SETROPTS options 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.<br>The TOE recognizes several authorities that are able to perform the different management tasks related to the TOE's security:<br>• General security options are managed by security administrators.<br>• 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. |

| TOE Security Functionality | Addressed issue |
|---|---|
| | • Users can change their own passwords or password phrases, their default groups, and their user names (but not their user IDs).<br>• Auditors manage the parameters of the audit system (a list of audited events, for example) and can analyze the audit trail.<br>• Security administrators can define what audit records are captured by the system.<br>• Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators. |
| Communication Security | z/OS provides means of secure communication between systems.<br>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 (TLS) encrypted communication for TCP/IP connections ( [TLSV1.1], [TLSV1.2]), 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.).<br>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 and AT-TLS 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.<br>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.<br>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) ([SSHV2])<br>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, specific network zones and individual ports on a per-application or per-user basis.<br>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 self protection | TSF protection is based on several protection mechanisms that are provided by the underlying abstract machine:<br>• Privileged processor instructions are only available to programs running in the processor's supervisor state<br>• Semi-privileged instructions are only available to programs running in an execution environment that is established and authorized by the TSF |

| TOE Security Functionality | Addressed issue |
|---|---|
| | • 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<br><br>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.<br><br>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.<br><br>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. |

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.4.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3, 3.2.3, and 3.4, respectively.

This certification covers the configurations of the TOE as outlined in chapter 8.

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 9, Para. 4, 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:

**z/OS,** Version 2 Release 1

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| z/OS Version 2 Release 1 (z/OS V2.1, program number 5650-ZOS) Common Criteria Evaluated Base Package | | | | |
| 1 | SW | z/OS V2.1 Common Criteria Evaluated Base<br>(IBM program number 5650-ZOS) | V2R1 | Tape |
| 2 | DOC | z/OS V2.1 Program Directory | GI11-9848-00 | Hardcopy |

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 3 | DOC | z/OS V2.1 Documentation Collection<br>Hashsum for download (ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/k4t49490.zip)<br>SHA256:<br>c8e55de4fc5d1ce72cf91bd8d1ffc4dd08ba9e3a8e030d77cd72ab595623d35b | | |
| 4 | DOC | ServerPac: IYO (Installing Your Order) | n/a | Hardcopy |
| 5 | DOC | Memo to Customers of z/OS V2.1 Common Criteria Evaluated Base | n/a | Hardcopy |
| 6 | DOC | z/OS V2.1 Planning for Multilevel Security and the Common Criteria | GA32-0891-00 | Hardcopy |
| IBM Print Services Facility™ Version 4 Release 4 for z/OS (PSF V4.4.0, program number 5655-M32) | | | | |
| 7 | SW | IBM Print Services Facility™ Version 4 Release 4 for z/OS (PSF V4.4.0, program number 5655-M32) | V4R4 | Tape |
| 8 | DOC | PSF V4.4 CDROM Library Collection | SK5T-8814-00 | CD-ROM |
| OGL/370 V1.1.0 (program number 5688-191) | | | | |
| 9 | SW | Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191) | V1R1 | Tape |
| 10 | DOC | OGL/370 V1.1.0: Getting Started | G544-3691-00 | Hardcopy |
| 11 | DOC | OGL/370 V1.1.0: LPS | G544-3697-00 | Hardcopy |
| 12 | DOC | OGL: Command Summary and Quick Reference | S544-3703-01 | Hardcopy |
| 13 | DOC | Program Directory OGL/370 | GI10-0212-01 | Hardcopy |
| IBM Ported Tools for z/OS V1.2 (program number 5655-M23) | | | | |
| 14 | SW | IBM Ported Tools for z/OS V1.2 (program number 5655-M23, optional) | V1.2 | Tape |
| 15 | DOC | Program Directory IBM Ported Tools for z/OS V1.2.0 | GI10-0769-06 | Hardcopy |
| 16 | DOC | IBM Ported Tools for z/OS License Information | GA22-7986-08 | Hardcopy |
| Additional Media | | | | |
| 17 | SW | PTFs for the following APARs (required):<br>OA41946, OA38971, OA41985, OA43423,<br>OA42093, OA41809, PM91543, OA43149,<br>OA42679, PM87944, OA43712, OA43935,<br>OA43539, OA43457, PI06650, OA43550, OA43536,<br>OA43350, OA43794, 0A43650, OA43812,<br>OA43741, OA43398<br>to be 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 ordered 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, CD-ROM and Documentation occurs in one package, which is manufactured specifically for this customer and shipped via courier services. Additional maintenance then needs to be downloaded by the customer via the ShopzSeries web site, following the instructions delivered with the package.

The download of the TOE guidance (see item #3 in Table 2 above) is described in the guidance [10] (see item #6 in Table 2 above), i.e. the customer downloads a guidance package from an IBM FTP Server and then verifies the package against the hashsums provided in the guidance or this report.

### 2.2. Identification of the TOE by the User:

The media and documents delivered to the customer are labeled with the product, document and version numbers as indicated in the table above and can be checked by the users installing the system. 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 operator command "`D IPLINFO`", to display the z/OS version. The string "*z/OS 02.01.00*" should be displayed among other information.

## 3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Identification and Authentication
- Discretionary Access Control
- Auditing
- Object Reuse
- Security Management
- Communication Security
- TSF self protection

## 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: Trained and trustworthy administrators, trusted remote IT, environmental support for protection of information, correct TOE setup, maintenance, prevention of physical attacks, recovery procedures and correct implementation of security protocols by the remote IT. Details can be found in the Security Target [6], section 4.2 and chapter 6.

## 5. Architectural Information

The Target of Evaluation (TOE) is the z/OS operating system with the software components as listed in table 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 a certified version of PR/SM on an IBM System z™ processor (zEnterprise 114, zEnterprise 196, or zEnterprise EC12) with CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement Feature 3863 active, with or without the zEnterprise BladeCenter Extension (zBX), optionally with CryptoExpress3 or CryptoExpress4 (zEC12 only) card.
- a certified version of IBM z/VM® executing in a logical partition provided by PR/SM on one of the above-listed System z™ processors.

If the configuration includes a zEnterprise BladeCenter Extension (zBX), the operating systems running in the zBX are not part of the TOE. They are external systems, connected to z/OS only via the built-in TCP/IP networking facilities included in the zEnterprise System and zBX.

Most of 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 exemption are cryptographic instructions implementing the AES, Triple-DES, SHA-1 and SHA-2 algorithms provided by the CPACF feature of the processor.

Cryptographic functions implemented by the (optional) CEX3 or CEX4 coprocessors are still part of the TOE environment and therefore have not been evaluated to the degree required by the target assurance level. In order to use only the cryptographic functions provided by the TOE a user needs to configure the TOE such that either no cryptographic coprocessor is installed or that the use of those functions is disabled.

A user that wants to use cryptographic functions provided by a coprocessor should be aware that although those functions have been tested during the evaluation for functional correctness, no further analysis of the design and implementation of those cryptographic functions implemented on the coprocessors has been performed. Especially no analysis for potentially exploitable side channels of the implementation of the cryptographic functions of the coprocessors has been performed.

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 instances of z/OS 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 Network Job Entry protocol.

Most of the TOE security functions are provided by the z/OS operating system Base Control Program 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 security status of the TOE.

# 6. Documentation

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

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

# 7. IT Product Testing

## 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" [11]. The hardware platforms implementing this abstract machine are:

- IBM zEnterprise 114 with CPACF DES/TDES Enablement Feature 3863 active , optionally with CryptoExpress3 card, and with or without the zEnterprise BladeCenter Extension (zBX).
- IBM zEnterprise 196 with CPACF DES/TDES Enablement Feature 3863 active, optionally with CryptoExpress3 card, and with or without the zEnterprise BladeCenter Extension (zBX).
- IBM zEnterprise zEC12 with CPACF DES/TDES Enablement Feature 3863 active, optionally with Crypto Express3 or Crypto Express4s card, and with or without the zEnterprise BladeCenter Extension (zBX).

Note that the above mentioned CryptoExpress cards are not part of z/OS and therefore the implementation of the cryptographic functions provided by those cards has not been analyzed. Testing has been performed using those cards to ensure that the cryptographic functions provided by those cards work in principle. No vulnerability analysis or side channel analysis for those cryptographic functions has been performed. The claims made in the Security Target concerning the cryptographic functions therefore apply to those functions implemented in software or by the CPACF feature.

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, section 1.4.3.2.

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 2 Release 1 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.

## 7.2. Developer Testing

This section provides a brief summary of the developer testing activities:

- 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.
- IBM has provided a common test framework for tests that can be automated. COMSEC is an environment that can be operated in standard mode or Labeled Security mode. The BERD (Background Environment Random Driver) test driver submits the testcases as JES2 jobs. IBM's intention is to move tests to this automated 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 2 release 1 in the evaluated configuration. The SDF team provided a pre-installed 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 successfully re-run.

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 Security Target [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 additional tests for enhancements of the already existing TOE components. All new test cases were determined to follow the approach of the already existing tests for the respective component.

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.

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 the standard mode and the Labeled Security mode 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 Version Security mode are compliant to standard mode 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 mode and standard mode configurations.

For test coverage the developer provided a mapping between the TSF of the Security Target [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 developer 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 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 IT environment of the TOE is accessed through the ICSF component.
- 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 details of the TOE design at the level of subsystems 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.

## 7.3. Evaluator Independent Testing

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 implicit testing of the Identification and authentication functions in TSO/E, ftp, su and JES, since these functions would be exercised extensively during the test activity by the testers. The tests focused on the Kerberos based authentication mechanisms. In addition the testers exercised the newly added sudo function with regard to I&A.
- 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 FACILITY class profiles was also performed.
- Communication security: The evaluators chose to ensure that secure communications channels (SSL, Kerberos and Intrusion Detections functions) 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-z/OS platform, checking different policy settings.
- Audit: 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 and observed, the evaluators chose an approach supplementing their own tests and focusing 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 [10].

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 [10], 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.

### 7.4. 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 concentrated his penetration testing on the only area where he identified a potential vulnerability (the NOSECURITY option when mounting a file system) and new potential side-channels in the software implementation of cryptographic algorithms. It can be easily seen that the only possible source of side-channels in a mainframe system is timing, since power analysis, emanation analysis, and fault injection can be excluded.

## 8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The z/OS V2R1 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 [10]. Also all required PTFs as listed as item #17 in table 2 above must be installed.

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).

The evaluated software configuration is not necessarily 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 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;

- In Labeled Security Mode, only the ICTX or LDBM configurations can be used. In standard mode the LDBM, CDBM, 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.

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

The SSH daemon sshd (from IBM Ported Tools for z/OS), may be used, but if used:

- must be configured to use protocol version 2 and either TDES 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 or public-key based authentication of users with the public keys stored in RACF keyrings. Rhost-based and public-key based user authentication with the keys stored elsewhere 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 SAFR_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 GSS-API 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 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.

TLS (Transport Layer Security) processing, if used, must use TLS V1.1 or TLS V1.2 protocols. TLS (Transport Layer Security), if used, must use one of the cipher suites listed in the FTP_ITC.1 SFR of the ST [6].

IPSec (IP Security) processing, if used, must use the ciphers listed in the FTP_ITC.1 SFR.

Any application performing client authentication using client digital certificates over 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 [10]:

- All Bulk Data Transfer (BDT) elements: BDT, BDT File-to-File , and BDT Systems Network Architecture (SNA) NJE
- The DFSTM Server Message Block (SMB) components of the Distributed File Service element
- Infoprint® Server
- JES3
- IBM Ported Tools for z/OS HTTP Server V7.0

In addition the following cannot be used in the certified configuration:

- The Advanced Program-to-Program Communication / Multiple Virtual Storage (APPC/MVS) component of the BCP
- The DFSMS Object Access Method for content management type applications
- The RACF remote sharing facility in remote mode.
- JES2 NJE communication via TCP/IP. JES2 NJE must use SNA or BSC in the certified configuration.
- JES2 Execution Batch Monitor (XBM) facility
- Most functions of Enterprise Identity Mapping (EIM). For details, see the manual z/OS Planning for Multilevel Security and the Common Criteria [10]

For the Communications Server:

- The z/OS FTP server and client, and the z/OS TN3270 server, support both manually-configured TLS, or AT-TLS. This evaluation has considered only AT-TLS configurations, and as a result manual configuration of those components to use 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, or the protocols from the formal RFC 4217 level of Security FTP with TLS [RFC4217]. 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: 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 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, and z/OS UNIX Trap Forwarder Daemon.

# 9. Results of the Evaluation

## 9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

The assurance refinements outlined in the PP [7] and the Security Target [6] were followed in the course of the evaluation of the TOE.

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

- All components claimed in the PP [7], Part 2: General Approach and Assurance Activities for OSPP Evaluations [12] and defined in the CC (see also part C of this report)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0874-2014, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was the conformance to General-Purpose Operating System Protection Profile Version 3.9, 6 December 2012, OSPP Technical Community [7].

The evaluation has confirmed:

- PP Conformance:
  General-Purpose Operating System Protection Profile Version 3.9, 6 December 2012, OSPP Technical Community [7]

- for the Functionality:
  PP conformant
  Common Criteria Part 2 extended
- for the Assurance:
  Common Criteria Part 3 conformant

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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

### System SSL

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| Protocol specifics | | | | | | |
| 1 | Trusted Channel | FTP_ITC.1 [ST], sec. 7.1.7.1<br>TLS v1.2 | [RFC5246]<br>(TLSv1.2)<br>and cf. all lines below | See below | yes<br>no | Security level depending on aggregated security level of the selected mechanisms as listed below. |
| 2 | Authenticity | RSA signature verification<br>(RSASSA-PKCS1-v1-5) using SHA-1 | [RFC3447] (PKCS#1 v2.1)<br>[FIPS180-4] (SHA) | Modulus length: 1024, 2048, 4096 | no | Verification of certificate signatures provided for authentication of peers.<br>Server and client certificates (optional) are used.<br>Algorithms used depending on the signature algorithm / hash algorithm used for signing the certificates and the accepted signature algorithms accepted by the peers.<br>Certificates are not generated by the TOE. |
| 3 | | RSA signature verification<br>(RSASSA-PKCS1-v1-5) using SHA-256, SHA-384) | [RFC3447](PKCS#1 v2.1)<br>[FIPS180-4] (SHA) | Modulus length: 2048, 4096 | yes | |
| 4 | | DSA signature verification using SHA-1 | [FIPS186-4] (DSA)<br>[FIPS-180-4] (SHA-1) | L= 1024<br>N= 160 | no | |
| 5 | | ECDSA signature verification using SHA-1 | [ANSI X9.62] (ECDSA),<br>[FIPS180-4] (SHA) | Key sizes corresponding to the used elliptic curve brainpoolP{224, | no | |

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| | | | | 256,320,384,512} r1 [RFC 5639] and secp{256,384,521}r1 [SEC2] | | |
| 6 | | ECDSA signature verification using SHA-256, SHA-384, SHA-512 | [ANSI X9.62] (ECDSA),<br><br>[FIPS180-4] (SHA) | Key sizes corresponding to the used elliptic curve brainpoolP{224, 256,320,384, 512} r1 [RFC 5639] and secp{256,384, 521}r1 [SEC2] | yes | |
| 7 | Authentication | RSA signature generation and verification<br><br>(RSASSA-PKCS1-v1-5 using SHA-1)<br><br>(TLS_DHE_DSS) | [RFC3447] (PKCS#1 v2.1) | Modulus length: 1024, 2048, 4096 | no | For Server depending on the cipher specified for keyexchange (& cert key usage).<br>For Client depending on the cert key usage).<br>Negotiated algorithms. |
| 8 | | RSA signature generation and verification<br><br>(RSASSA-PKCS1-v1-5 using SHA-256, SHA-384)<br><br>(TLS_DHE_RSA) | [RFC3447] (PKCS#1 v2.1) | Modulus length: 1024 | no | |
| | | | | Modulus length: 2048, 4096 | yes | |
| 9 | | DSA signature generation and verification using SHA-1<br><br>(TLS_DHE_DSS) | [FIPS186-4] (DSA) [FIPS-180-4] (SHA-1)<br>[RFC5246] (TLSv1.2 | plength= 1024<br>qlength= 160 | no | |
| 10 | | ECDSA signature generation and verification using SHA-1<br><br>(TLS_ECDHE_ECDSA) | [ANSI X9.62] (ECDSA),<br><br>[FIPS180-4] (SHA),<br><br>[RFC4492] (ECC for TLS) | Key sizes corresponding to the used elliptic curve brainpoolP{224, 256,320,384,512} r1 [RFC 5639] and secp{256,384,521}r1 [SEC2] | no | |

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| 11 | | ECDSA signature generation and verification using SHA-256, SHA-384<br><br>(TLS_ECDHE_ECDSA) | [ANSI X9.62] (ECDSA),<br><br>[FIPS180-4] (SHA),<br><br>[RFC4492] (ECC for TLS) | Key sizes corresponding to the used elliptic curve brainpoolP{224, 256,320,384, 512} r1 [RFC 5639] and secp{256,384, 521}r1 [SEC2] | yes | |
| 12 | | HMAC with SHA-256, SHA-384 | [RFC2104] (HMAC)<br><br>[FIPS180-4] (SHA)<br><br>[RFC5246] (TLSv1.2) | \|k\| = 256, 384 | yes | Finished message (TLS handshake) |
| 13 | Key establishment | RSA (TLS_RSA)<br><br>RSA encryption (client) and decryption (server) (RSAES-PKCS1-v1-5) | [RFC3447] (PKCS#1 v2.1) | Modulus size 1024 | no | |
| | | | | Modulus size 2048, 4096 | yes | |
| 14 | | DH / DHE<br><br>(TLS_DH_, TLS_DHE) | [RFC2631] | Groups with modulus size 1024 | no | |
| | | | | Modulus size 2048, 4096 | yes | |
| 15 | | ECDHE<br><br>(TLS_ECDHE_) | [RFC4492] (ECC for TLS)<br><br>[TR-03111] (ECC) | Key sizes corresponding to the used elliptic curve brainpoolP{224, 256,320,384, 512} r1 [RFC 5639] and secp{256,384, 521}r1 [SEC2] | yes | |
| 16 | Confidentiality | AES in CBC and GCM mode<br><br>(AES_{128\|256}_{CBC\|GCM}) | [FIPS197] (AES)<br><br>[SP800-38A] (CBC)<br><br>[SP800-38D] (GCM)<br><br>[RFC5289] (Elliptic Curve Cipher Suites with SHA-256/384 and AES (GCM) | \|k\| = 128, 256 | yes | CPACF (bulk data encryption record layer)<br><br>GCM – authenticated encryption |
| 17 | Integrity & authenticity | HMAC with SHA-1 or SHA-256 or SHA-384)<br><br>(SHA), (SHA256), (SHA384) | [RFC2104] (HMAC<br><br>[FIPS180-4] (SHA) | \|k\| = 160, 256, 384 | yes | CPACF (message authentication record lay |

## OpenSSH

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| 1 | Trusted Channel | FTP_ITC.1 [ST], sec. 7.1.7.1<br>SSH v2 | [RFC4250] (lists the RFCs defining SSH V2):<br>RFC 4251,<br>RFC 4252,<br>RFC 4253,<br>RFC 4254 | See below | yes<br>no | Security level depending on aggregated security level of the selected mechanisms as listed below. |
| 2 | Authentication | RSA signature generation & verification<br>RSASSAPKCS1-v1_5 using SHA-1<br>(ssh-rsa) | [RFC3447] (PKCS#1 v2.1)<br>[FIPS-180-4] (SHA-1)<br>[RFC4253] (SSH-TRANS) for host authentication<br>[RFC4252], sec 7 (SSH-USERAUTH) for user authentication<br>method: “publickey” | Modulus length: 1024, 2048 and 4096 | no | Pubkeys are exchanged trustworthy out of band.<br>Authenticity is not part of the TOE. |
| 3 | | DSA signature generation & verification using SHA-1<br>(ssh-dss) | [FIPS186-4] (DSA)<br>[FIPS-180-4] (SHA-1)<br>[RFC4253] (SSH-TRANS) for host authentication<br>[RFC4252], sec 7 (SSH-USERAUTH) for user authentication<br>method: “publickey” | L= 1024<br>N= 160 | no | |
| 4 | Key establishment | DH-Group1-SHA1 | RFC4253] (SSH-TRANS) supported by [RFC2409] (DH groups IKE)<br>[FIPS-180-4] (SHA-1) | plength 1024 | no | |
| 5 | | DH-Group14-SHA1 | [RFC4253] (SSH-TRANS) supported by [RFC3526] (DH groups IKE)<br>[FIPS-180-4] (SHA-1) | plength=2048 | yes | |
| 6 | Confidentiality | AES128-CBC<br>AES192-CBC<br>AES256-CBC | [FIPS-197] (AES),<br>[SP 800-38A] (CBC), | \|k\| = 128, 192, 256 | yes | Binary packet protocol: encryption |
| 7 | | 3DES-CBC | [FIPS46-3] (DES)<br>[SP 800-67] (TDES/TDEA) | \|k\| = 168 | yes | |
| 8 | Integrity & authenticity | HMAC-SHA1<br>HMAC-SHA1-96 | [FIPS 180-2] (SHA),<br>[RFC 2104] (HMAC) | \|k\| = 160 | yes | Binary packet protocol: message authentication |
| 9 | | HMAC-MD5 | [RFC1321] (MD5), | \|k\| = 128 | yes | |

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| | | HMAC-MD5-96 | [RFC2104] (HMAC), [RFC4253] (SSH v2.0) | | | |

Table 3.2: TOE cryptographic functionality

## IPSec / IKE

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| 1 | Trusted Channel | FTP_ITC.1 [ST], sec. 7.1.7.1<br>IKEv1, IKEv2, IPsec | [RFC4301] (IPSec), [<br>RFC4303] (ESP),<br>[RFC2409] (IKEv1), [RFC5996] (IKEv2) | See below | yes<br>no | Security level depending on aggregated security level of the selected mechanisms as listed below. |
| 2 | Authenticity | RSA signature verification<br>(RSASSA-PKCS1-v1-5) using SHA-1 | [RFC3447] (PKCS#1 v2.1)<br>[FIPS180-4] (SHA) | Modulus length: 1024, 2048, 4096 | no | Certificate signature verification.<br>See also system SSL. |
| 3 | | RSA signature verification<br>(RSASSA-PKCS1-v1-5) using SHA-256, SHA-384) | [RFC3447] (PKCS#1 v2.1)<br>[FIPS180-4] (SHA) | Modulus length: 2048, 4096 | yes | |
| 4 | | DSA signature verification using SHA-1 | [FIPS186-4] (DSA) [FIPS-180-4] (SHA-1) | L= 1024<br>N= 160 | no | |
| 5 | | ECDSA signature verification using SHA-1 | [ANSI X9.62] (ECDSA),<br>[FIPS180-4] (SHA) | Key sizes corresponding to the used elliptic curve brainpoolP{224, 256,320,384,512} r1 [RFC 5639] and secp{256,384,521}r1 [SEC2] | no | |
| 6 | | ECDSA signature verification using SHA-256, SHA-384, SHA-512 | [ANSI X9.62] (ECDSA),<br>[FIPS180-4] (SHA) | Key sizes corresponding to the used elliptic curve brainpoolP{224, 256,320,384, 512} r1 [RFC 5639] and secp{256,384, 521}r1 [SEC2] | yes | |
| 7 | Authentication | RSA signature generation and | [RFC2409] (IKEv1), | Modulus length 1024 | no | |

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| | | verification for authentication (Auth. Method 1)<br><br>**IKEv1**: RSAES-PKCS1-v1_5 encryption scheme with private key encryption for signing and public keydecryption for signature. verification. | [RFC3447] (PKCS#1 v2.1) | Modulus length 2048, 4096 | yes | |
| | | ECDSA (secp{224, 256, 384, 521}r1, brainpoolP{224, 256, 320, 384, 512}r1) | PKCS#1 v2.1, FIPS180-4 (SHA), RFC5996 (IKEv2) | \|k\| = 224, 256, 320, 384, 512, 521 | yes | |
| 8 | | RSA signature generation + verification (Auth Method 1)<br><br>**IKEv2**: RSASSA-PKCS1-v1_5) using SHA-1 | [5996] (IKEv2)<br>[RFC3447] (RSA) | Modulus length:<br>1024<br>2048,<br>4096 | no | |
| 9 | | ECDSA signature generation + verification using one of SHA-256, SHA-384, SHA-512<br><br>(ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521) | [RFC4754] ECDSA within IKEv1 and IKEv2<br><br>[5903] ECP groups<br><br>[ANSI X9.62] (ECDSA),<br><br>[FIPS180-4] (SHA), | Key sizes corresponding to the used elliptic curves secp256, 384, 521}r1 ([SEC2]) | yes | |
| 10 | Key establishment (key agreement) | DH with DH groups:<br>1,2,5 | [RFC2409] (IKEv1), [RFC5996] (IKEv2),<br>[DH] (DH as referenced in [RFC2409] & [RFC5996]) | plength<br>= 1024, 1024, 1534 | no | |
| 11 | | 14 (2048-bit MODP), | [RFC3526] | plength=2048 | yes | |
| 12 | | 24 (2048-bit MODP with 256-bit POS),<br>MODP with subgroups | [RFC5114] | plength = 2048<br>(256) | yes | |
| 13 | | 19 (256-bit elliptic curve),<br>20 (384-bit elliptic curve),<br>21 (521-bit elliptic curve) | [RFC5114] | plength<br>= 256, 384, 521 | yes | |

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits | Comments |
|---|---|---|---|---|---|---|
| 14 | Confidentiality (bulk encryption) | AES-CBC-128<br>AES-CBC-256<br>AES-GCM-128<br>AES-GCM-256 | RFC 4106:<br><br>[FIPS-197] (AES),<br>[SP 800-38A] (CBC),<br>[RFC3602] (AES-CBC with ESP),<br>[RFC5996] (IKv2) | \|k\| = 128, 256 | yes | IKE ESP / IPSec ESP |
| 15 | Integrity & authenticity | HMAC-SHA1-96<br>AES-XCBC-MAC-96 | [FIPS180-4] (SHA),<br>[RFC2104] (HMAC),<br>[RFC2404] (HMAC-SHA-1-96),<br>[RFC5996] (IKEv2)<br><br>[FIPS-197] (AES),<br>[RFC3566] (XCBC-MAC),<br>[RFC5996] (IKEv2) | \|k\| = 160, 128 | yes | |

Table 3.3: TOE cryptographic functionality

# 10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

# 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

**AIS** Application Notes and Interpretations of the Scheme

| | |
|---|---|
| **APF** | Authorized program facility |
| **AT-TLS** | Application-Transparent TLS |
| **BCP** | Base Control Program |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **CEM** | Common Methodology for Information Technology Security Evaluation |
| **CEX** | CryptoExpress |
| **CMP** | Certificate Management Protocol |
| **CN** | Common Name |
| **CPACF** | CP Assist for Cryptographic Functions |
| **DAC** | Discretionary access control |
| **DFSMS** | Data Facility Storage Management Subsystem |
| **DIT** | Directory Information Tree |
| **DN** | Distinguished Name |
| **EAL** | Evaluation Assurance Level |
| **ECC** | Elliptic Curve Cryptography |
| **ETR** | Evaluation Technical Report |
| **FVT** | Functional Verification Tests |
| **ICR** | Identity Context Reference |
| **ICSF** | Integrated Cryptographic Services Facility |
| **ICTX** | Identity Context Extension |
| **IKE** | Internet Key Exchange |
| **IOCDS** | Input/Output configuration Data Set |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **JCL** | Job Control Language |
| **JES** | Job Entry System |
| **LDAP** | Lightweight Directory Access Protocol |
| **LDBM** | Lightweight Database Manager |
| **MAC** | Mandatory Access Control |
| **MVS** | Multiple Virtual Storage |
| **NSS** | Network Security Service |
| **PADS** | Program Access to Data Sets |

| | |
|---|---|
| **PDSE** | Partitioned Data Set Extended |
| **PKCS** | Public Key Cryptographic Standard |
| **PKI** | Public Key Infrastructure |
| **PKM** | Program Key Mask |
| **POSIX** | Portable Operating System Interface for UNIX |
| **PP** | Protection Profile |
| **PR/SM™** | Processor Resource/Systems Manager™ |
| **PTF** | Program Temporary Fix |
| **RACF** | Resource Access Control Facility |
| **SAF** | System Authorization Facility |
| **SAR** | Security Assurance Requirement |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SMF** | System Management Facilities |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TLS** | Transport Layer Security |
| **TSO** | Time Sharing Option |
| **TSF** | TOE Security Functions |
| **VTOC** | Volume Table of Content |

## 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 TOE-protected objects.

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

**Package** - A named set of either functional or assurance requirements (e.g. EAL 3).

**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 non-hierarchical 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** - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

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

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

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

**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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (BSI 7125)

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

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

[6] Security Target BSI-DSZ-CC-0972-2015, Version 1.7, 17. July 2015, Security Target for IBM z/OS Version 2 Release 1 for Compliance with the NIAP/BSI OSPP, IBM Corporation

[7] General-Purpose Operating System Protection Profile Version 3.9, 6 December 2012, OSPP Technical Community

[8] Final Evaluation Technical Report, Version 3, 08. April 2015 , atsec information security GmbH, (confidential document)

[9] Configuration list for the TOE, 2014-04-01, file name: CM.LISTS-V2R1.zip and Configuration List for the Publications, CM.PUBS-V2R1.txt (confidential documents)

[10] MLSGUIDE z/OS Planning for Multilevel Security and the Common Criteria, Version GA32-0891-00, April 2014

[11] z/Architecture Principles of Operation, Tenth Edition, Version SA22-7832-09, September 2012.

[12] General-Purpose Operating System Protection Profile - Part2: General Approach and Assurance Activities for OSPP Evaluations Version 3.9, OSPP Technical Community

[8] specifically

- AIS 20, Version 3, 15 May 2013, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, 28 September 2007, Reuse of evaluation results

# C. Excerpts from the Criteria

CC Part 1:

**Conformance Claim** (chapter 10.4)

“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 D.”

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<br>APE_OBJ.2 Security objectives |
| | APE_ECD.1 Extended components definition |
| | APE_REQ.1 Stated security requirements<br>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<br>ASE_OBJ.2 Security objectives |
| | ASE_ECD.1 Extended components definition |
| | ASE_REQ.1 Stated security requirements<br>ASE_REQ.2 Derived security requirements |
| | ASE_TSS.1 TOE summary specification<br>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 decomposition.

| Assurance Class | Assurance Components |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.1 Basic functional specification<br>ADV_FSP.2 Security-enforcing functional specification<br>ADV_FSP.3 Functional specification with complete summary<br>ADV_FSP.4 Complete functional specification<br>ADV_FSP.5 Complete semi-formal functional specification with additional error information<br>ADV_FSP.6 Complete semi-formal functional specification with additional formal specification |
| | ADV_IMP.1 Implementation representation of the TSF<br>ADV_IMP.2 Implementation of the TSF |
| | ADV_INT.1 Well-structured subset of TSF internals<br>ADV_INT.2 Well-structured internals<br>ADV_INT.3 Minimally complex internals |
| | ADV_SPM.1 Formal TOE security policy model |
| | ADV_TDS.1 Basic design<br>ADV_TDS.2 Architectural design<br>ADV_TDS.3 Basic modular design<br>ADV_TDS.4 Semiformal modular design<br>ADV_TDS.5 Complete semiformal modular design<br>ADV_TDS.6 Complete semiformal modular design with formal high-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<br>ALC_CMC.2 Use of a CM system<br>ALC_CMC.3 Authorisation controls<br>ALC_CMC.4 Production support, acceptance procedures and automation<br>ALC_CMC.5 Advanced support |
| | ALC_CMS.1 TOE CM coverage<br>ALC_CMS.2 Parts of the TOE CM coverage<br>ALC_CMS.3 Implementation representation CM coverage<br>ALC_CMS.4 Problem tracking CM coverage<br>ALC_CMS.5 Development tools CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures<br>ALC_DVS.2 Sufficiency of security measures |
| | ALC_FLR.1 Basic flaw remediation<br>ALC_FLR.2 Flaw reporting procedures<br>ALC_FLR.3 Systematic flaw remediation |
| | ALC_LCD.1 Developer defined life-cycle model |

| Assurance Class | Assurance Components |
|---|---|
| | ALC_LCD.2 Measurable life-cycle model |
| | ALC_TAT.1 Well-defined development tools<br>ALC_TAT.2 Compliance with implementation standards<br>ALC_TAT.3 Compliance with implementation standards - all parts |
| ATE: Tests | ATE_COV.1 Evidence of coverage<br>ATE_COV.2 Analysis of coverage<br>ATE_COV.3 Rigorous analysis of coverage |
| | ATE_DPT.1 Testing: basic design<br>ATE_DPT.2 Testing: security enforcing modules<br>ATE_DPT.3 Testing: modular design<br>ATE_DPT.4 Testing: implementation representation |
| | ATE_FUN.1 Functional testing<br>ATE_FUN.2 Ordered functional testing |
| | ATE_IND.1 Independent testing – conformance<br>ATE_IND.2 Independent testing – sample<br>ATE_IND.3 Independent testing – complete |
| AVA: Vulnerability assessment | AVA_VAN.1 Vulnerability survey<br>AVA_VAN.2 Vulnerability analysis<br>AVA_VAN.3 Focused vulnerability analysis<br>AVA_VAN.4 Methodical vulnerability analysis<br>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.

**Evaluation assurance level 1 (EAL 1) - functionally tested** (chapter 8.3)

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested** (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked** (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed** (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested** (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested** (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested** (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 |
| 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 | 1 | 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”

**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.”

# D. Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.