Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/22

(Certification No.)

Prodotto: IBM z/OS Version 2 Release 4

(Product)

Sviluppato da: IBM Corporation

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 13 gennaio 2022

Fino a EAL2 *(Up to EAL2)*

Common Criteria

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM z/OS Version 2 Release 4

OCSI/CERT/ATS/03/2020/RC

Version 1.0

13 January 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	13/01/2022

2 Table of contents

3 Acronyms

ABEND	Abnormal End
AES	Advanced Encryption Standard
AKM	Access Key Mask
APAR	Authorized Program Analysis Report
APF	Authorized Program Facility
API	Application Programming Interface
APPC/MVS	Advanced Program-to-Program Communication / Multiple Virtual Storage
AT-TLS	Application Transparent Transport Layer Security
BCP	Base Control Program
BDT	Bulk Data Transfer
BERD	Background Environment Random Driver
BSC	Binary Synchronous Communication
CA	Certificate Authority
CC	Common Criteria
CCEB	Common Criteria Evaluated Base
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPACF	Central Processor Assist for Cryptographic Function
CVE	Common Vulnerabilities and Exposures
DES	Data Encryption Standard
DFS	Distributed File Service
DFSMS	Data Facility Storage Management Subsystem
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
EIM	Enterprise Identity Mapping

ETR	Evaluation Technical Report
FTP	File Transfer Protocol
FVT	Functional Verification Tests
HASP	Houston Automatic Spooling Priority
HMAC	Keyed-hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICSF	Integrated Cryptographic Service Facility
ID	Identifier
IKE	Internet Key Exchange
IP	Internet Protocol
IPD	Integrated Product Development
IPL	Initial Program Load
IPSec	IP Security
IT	Information Technology
JES	Job Entry System
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NJE	Network Job Entry
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System
PC	Program Call
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
PR/SM	Processor Resource/System Manager
PTF	Program Temporary Fix

RACF	Resource Access Control Facility
RFC	Request for Comments
RRSF	RACF Remote Sharing Facility
SAK	System Assurance Kernel
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMB	Server Message Block
SMF	System Management Facilities
SNA	Systems Network Architecture
SHA	Secure Hash Algorithm
SSH	Secure SHell
ST	Security Target
SVC	Supervisor Call
SVT	System Verification Tests
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple DES
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSO	Time Sharing Option
TSO/E	TSO Extensions
UID	User Identifier
USS	UNIX System Services
XBM	Execution Batch Monitor

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

4.2 Technical documents

[CR] Certification Report “IBM z/OS Version 2 Release 3”, OCSI/CERT/ATS/01/2018/RC, version 1.0, 31 July 2019

[ETRv1] Final Evaluation Technical Report “IBM z/OS Version 2 Release 4”, Version 1, atsec information security GmbH, 20 October 2021

[ETRv2] Final Evaluation Technical Report “IBM z/OS Version 2 Release 4”, Version 2, atsec information security GmbH, 10 January 2022

[GPOSPP] Protection Profile for General Purpose Operating Systems, NIAP, Version 4.2.1, 22 April 2019

[MLSGUIDE] “z/OS V2.4 - Planning for Multilevel Security and the Common Criteria”, GA32-0891-40, 23 May 2021

[OSPP] Operating System Protection Profile, Version 2.0, BSI-CC-PP-0067, 1st June 2010

[OSPP-EIA] OSPP Extended Package – Extended Identification and Authentication, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[OSPP-LS] OSPP Extended Package – Labeled Security, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[ST] “IBM z/OS Version 2 Release 4 Security Target”, Version 1.3, IBM Corporation, 10 January 2022

[ZARCH] “z/Architecture Principles of Operation”, SA22-7832-12, September 2019

5 Recognition of the certificate

5.1 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “IBM z/OS Version 2 Release 4”, also referred to in the following as z/OS V2R4 or z/OS, developed by International Business Machines Corp. (IBM).

The TOE is a general-purpose, multi-user, multi-tasking operating system for enterprise computing systems.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (IBM z/OS Version 2 Release 3), already certified by OCSI (Certificate no. 6/19 of July 31, 2019 [CR]).

Due to some changes made to the product by the Developer IBM Corp., it was deemed necessary to undertake a re-certification of the TOE. Namely, a number of security functions and services of the TOE in V2R3 are no longer comprised in the scope of the TOE in V2R4. In addition, the new version of the TOE in V2R4 no longer claims conformance to [OSPP] and relevant extended packages ([OSPP-EIA], [OSPP-LS]) or to other PPs. However, the LVS atsec information security GmbH was able to reuse part of the documentation and evidences already provided in the previous evaluation.

Note that the changes have also led to the revision of the Security Target [ST]. Customers of the previous version of the TOE are therefore advised to take also into account the new ST.

While the considerations and recommendations already expressed for the previous TOE remain largely valid, for ease of reading this Certification Report has been rewritten in its entirety so as to constitute an autonomous document associated with the new TOE “IBM z/OS Version 2 Release 4”.

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_FLR.3, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “IBM z/OS Version 2 Release 4” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	IBM z/OS Version 2 Release 4
Security Target	IBM z/OS Version 2 Release 4 Security Target, Version 1.3 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security GmbH
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	21 May 2020
Evaluation ending date	20 October 2021

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are met.

7.3 Evaluated product

This paragraph summarizes the main functional and security features of the TOE; for a detailed description, refer to the Security Target [ST].

The TOE is the software product z/OS Version 2 Release 4 (V2R4), including accompanying documentation and SW APARs as detailed in Table 2.

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 a more detailed description of the TOE, please refer to sect. 1.5 (“TOE description”) of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

7.3.1.1 TOE general overview

The TOE is the z/OS operating system with the software components as listed in Table 2.

The TOE is one instance of z/OS running on an abstract machine as the sole operating system and exercising full control over this abstract machine. This abstract machine, the most of which not being part of the TOE as described below, can be provided by one of the following:

- a logical partition provided by a certified version of PR/SM running on IBM z15 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express7S cards;
- a certified version of IBM z/VM® executing in a logical partition provided by PR/SM on System z™ processors.

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.

Individual TOEs can be run alone or within a network as a set of cooperating hosts, operating under and implementing the same set of security policies. They also can be connected to form a loosely-coupled complex of systems called a sysplex.

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

Some elements have been included in the TOE that do not provide security functions. These elements run in authorized mode, so they can 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 requires they undergo a process of scrutiny during the evaluation which ensures that they may be used by customers without affecting the TOE’s security.

7.3.1.2 Major software components of the TOE

z/OS Version 2 Release 4 includes the following main subsystems:

- **Base Control Program (BCP)**: BCP is the core subsystem of z/OS responsible for (real and virtual) storage management, management of address spaces, tasks and SRBs, scheduling, handling of interrupts and exceptions, synchronization and other basic services.

- **System Management Facilities (SMF)**: SMF collects and records system and job-related information that the installation can use for: billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, maintaining system security.

- **Data Facility Storage Management Subsystem (DFSMS)**: System-managed storage is the IBM automated approach to managing storage resources. It uses software programs to manage data security, placement, migration, backup, recall, recovery, and deletion so that current data is available when needed, space is made available for creating new data and for extending current data, and obsolete data is removed from storage.

- **Resource Access Control Facility (RACF)**: RACF is the central component within z/OS responsible for the identification and authentication of users, for access control, and for the generation of security event related audit records (which RACF sends to SMF to get those audit records included in the SMF audit).

- **Integrated Cryptographic Service Facility (ICSF)**: ICSF is the main provider of basic cryptographic services within z/OS and for the functions specified in the SFRs. It is utilized for the basic cryptographic services for certificate/key generation for certificates used for user authentication as well as certificates used in the establishment of trusted channels.

- **Communications Server**: The Communications Server component of z/OS is responsible for the implementation of the TCP/IP stack and the higher level protocols (except for SSH). As security functionality the Communications Server provides: access control on the objects, trusted channels, IP filtering capabilities.

- **Job Entry Subsystem 2 (JES2)**: z/OS uses a job entry subsystem (JES) to receive jobs into the operating system, schedule them for processing by z/OS, and to control their output processing. JES2 is descended from HASP (Houston Automatic Spooling Priority). HASP is defined as a computer program that provides supplementary job management, data management, and task management functions such as scheduling, control of job flow, and spooling.

- **Time Sharing Option (TSO/E)**: TSO/E is the primary user interface to the z/OS system. TSO/E provides numerous commands for both end users and system programmers that allow them to interact with TSO/E and the z/OS system.

- **UNIX System Services (USS)**: The z/OS support for z/OS UNIX enables two open systems interfaces on the z/OS operating system: an application programming interface (API), which is XPG4 UNIX 1995 conforming and an interactive z/OS shell interface.

- **OpenSSH**: Secure Shell (SSH) is a network protocol which provides an alternative for insecure remote login and command execution facilities, such as telnet, rlogin and rsh. SSH encrypts traffic in both directions, preventing traffic sniffing and password theft. The SSH that is provided for z/OS is a port of OpenSSH 6.4p1, available from www.openssh.org.

7.3.2 TOE security features

7.3.2.1 Security policy

The primary security features of the TOE are:

- identification and authentication;
- discretionary access control;
- auditing;
- object reuse;
- security management;
- secure communication;
- TSF protection;
- confidentiality protection of data sets.

They are supported by domain separation and reference mediation, which ensure that the features are always invoked and cannot be bypassed.

7.3.2.2 Operational environment security objectives

The Assumptions for the correct operation of the TOE are defined in section 3.3 of the Security Target [ST]. The following objectives for the operational environment have to be assured:

- The OS is installed on trusted hardware.
- The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
- The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.
- If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.
- Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.

- Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.

- The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.

For a complete description of the security objectives for the TOE operational environment, please refer to sect. 4.2 of the Security Target [ST].

7.3.2.3 Security functions

For a detailed description of the TOE Security Functions, consult sect. 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Identification and Authentication**: z/OS provides various methods for identification and authentication of users.

- **Discretionary Access Control**: z/OS supports access controls that are capable of enforcing access limitations on individual users and data objects; 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.

- **Communication Security**: z/OS provides different means of secure communication between systems sharing the same security policy, including trusted communication channels for TCP/IP connections, supports the SSH v2 protocol, the IP Security (IPSec) protocol with Internet Key Exchange (IKE).

- **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, and general resource profiles.

- **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.

- **Object Reuse**: reuse of protected objects and of storage is handled by various hardware and software controls, and by administrative practices.

- **TSF Protection**: TSF protection is based on several protection mechanisms that are supported by the underlying abstract machine z/OS is executed upon.

- **Confidentiality Protection of Data Sets**: with z/OS confidentiality protection of data sets, users can encrypt data at rest without requiring application changes.

7.3.3 Cryptographic functions

Cryptographic functions implemented by the CEX7S coprocessors are part of the TOE environment and therefore have not been evaluated to the degree required by the target assurance level. It should be noted that a cryptographic coprocessor is required to operate the TOE in its evaluated configuration.

A user who 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.

The claims made in the Security Target concerning the cryptographic functions therefore apply to those functions implemented in software or by CPACF.

The Cryptographic Functions are detailed in section 6.1.2 of the Security Target ([ST]). Section 5.1 also defines extended components for cryptographic support.

7.4 Documentation

The guidance documentation specified in Annex A - Guidelines for secure usage of the TOE is delivered to the customer together with the product. The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFRs) have been selected or derived by extension from CC Part 2 [CC2].

All of the extended requirements defined in the Security Target [ST] have been drawn from the PP [GPOSPP], although the ST does not declare conformance to this PP. The SFRs originating from [GPOSPP] are distinguishable from CC Part 2 SFRs by the ending “_EXT” or having the term “(Refined)” appended.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize such objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially, the Security Target has been evaluated to ensure that it constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body (OCSI) has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security GmbH.

The evaluation was completed on 20 October 2021 with the issuance by LVS of the Evaluation Technical Report [ETRv1]. An updated version of the ETR ([ETRv2]) containing only minor revisions was approved by the Certification Body on 12 January 2022. Then, the Certification Body issued this Certification Report.

7.8 General considerations on the validity of the certification

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist. It remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report ([ETRv1] and [ETRv2]), issued by the LVS atsec information security GmbH, and the documents required for the certification, and considering the evaluation activities which was carried out, the Certification Body (OCSI) concluded that TOE "IBM z/OS Version 2 Release 4" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_FLR.3.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Systematic flaw remediation	*ALC_FLR.3*	Pass
Tests	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing – sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (“Statement of Certification”).

Potential customers of the product “IBM z/OS Version 2 Release 4” are suggested to properly understand the specific purpose of the certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in section 4.2 of the Security Target [ST]. Potential customers are advised to check that they meet the identified requirements and to pay attention to the recommendations contained in this Report.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A - Guidelines for secure usage of the TOE includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([MLSGUIDE]).

It is assumed that the TOE operates securely if the assumptions about the operational environment described in section 3.3 of the Security Target [ST] are satisfied. In particular, it is assumed that the administrators of the TOE are adequately trained to the correct usage of the TOE and chosen among the trusted personnel of the organization. The TOE is not designed to counter threats from unexperienced, malicious or negligent administrators.

It should also be noted that TOE security is conditioned by the proper functioning of the software and hardware platforms on which the TOE is installed, and of all trusted external

IT systems supporting the implementation of TOE's security policy. Specifications for the operational environment are described in the Security Target [ST].

9 Annex A - Guidelines for secure usage of the TOE

This Annex provides considerations particularly relevant to the potential customers of the TOE.

9.1 TOE delivery

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.

Table 2 contains the items that comprise the different elements of the TOE, including software and guidance.

#	Type	Identifier	Release	Form of delivery
z/OS Version 2 Release 4 (z/OS V2.4, program number[1] 5650-ZOS) Common Criteria Evaluated Base Package				
1	SW	z/OS V2.4 Common Criteria Evaluated Base (IBM program number 5650-ZOS)	V2R4	Tape
2	DOC	z/OS V2.4 Program Directory	GI11-9848-03	Hardcopy
3	DOC	z/OS V2R4 Library V2R4 Archive file name: zOSV2R4Library.zip	V2R4	Electronic
		Download from: https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4Library "Download all z/OS V2R4 Library publications to ZIP file"		
4	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
5	DOC	Memo to Customers of z/OS V2.4 Common Criteria Evaluated Base	n/a	Hardcopy
6	DOC	z/OS V2.4 Planning for Multilevel Security and the Common Criteria File name: e0ze100_v2r4.pdf Last updated: 2021-05-23 SHA256 checksum: 65cd99fb8f96d18ea6b2f2a7e7d2a4dae6b4c8c39cf615908cda4d1bf9f8c3ba	GA32-0891-40	Electronic
Additional Media				
7	SW	PTFs for the following APARs (required): • OA57641 (PTF UJ02099) • OA57934 (PTF UJ00393) • OA58067 (PTF UJ02223) • OA58074 (PTF UJ02931) • OA58282 (PTF UJ01931) • OA58313 (PTF UJ02442) • OA58349 (PTF UJ02614) • OA58505 (PTF UJ01875)	n/a	Electronic

[1] The “program number” (or “product number”) is IBM's technical identification of the product “z/OS”. It is used for order and license purposes and does not uniquely identify the TOE. The string “z/OS Version 2 Release 4” uniquely identifies the TOE.

#	Type	Identifier	Release	Form of delivery
		• OA58588 (PTF UJ01732) • OA58595 (PTF UJ01957) • OA58781 (PTF UJ01929 & PTF UJ01933) • OA58990 (PTF UJ02368 & PTF UJ02370) • OA59021 (PTF UJ02052) • OA59040 (PTF UJ02630) • OA59074 (PTF UJ02508 & PTF UJ02509) • OA59156 (PTF UJ02505) • OA59268 (PTF UJ02741 & PTF UJ02741) • PH14146 (PTF UI68531) • PH14509 (PTF UI66980) • PH14511 (PTF UI67180) These PTFs are to be obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)		

Table 2 - TOE Deliverables

The delivery of all media occurs in one package, which is manufactured specifically for customers 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.

Electronic delivery of the guidance is provided through the IBM web site at https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4Library. Users can retrieve the whole guidance package for the TOE (see item #3 in Table 2) by clicking the link “Download all z/OS V2R4 Library publications to ZIP file”. The download is protected by the HTTPS protocol and can be verified by users by clicking on the lock symbol in their browser’s address field to verify the IBM certificate. The resulting ZIP archive named zOSV2R4Library.zip will also contain the manual [MLSGUIDE] (see item #6 in Table 2), which contains further instructions on how to set up the TOE in its evaluated configuration.

9.2 Identification of the TOE

The media delivered to the customer are labeled with the product, document and version numbers as indicated in Table 2 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 02.04.00” should be displayed among other information.

9.3 Installation, initialization and secure usage of the TOE

9.3.1 Software installation and configuration

The Target of Evaluation is IBM z/OS, Version 2 Release 4. The TOE is software only and is accompanied by guidance documentation. The items listed in Table 2 represent the TOE.

The z/OS V2R4 Common Criteria Evaluated Base package must be installed according to the directions delivered with the media and configured according to the instructions in chapter 7 of [MLSGUIDE]. Also, all required PTFs as listed as item #7 in Table 2 must be installed.

During installation it is possible to choose not to use any of the elements delivered within the ServerPac, but installation, configuration and use of at least the RACF component of the z/OS Security Server element is required.

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;
- using the Authorized Caller Table (ICHAUTAB) in RACF to allow unauthorized programs to issue RACROUTE REQUEST=VERIFY (RACINIT) or RACROUTE REQUEST=LIST (RACLIST).

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

The SSH daemon `sshd` may be used, but if used:

- must be configured to use protocol version 2 and one of the AES-based cipher 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.

TLS:

- TLS (Transport Layer Security) processing, if used, must use TLS V1.2 or TLS V1.3 protocols. TLS, if used, must use one of the cipher suites listed in the FCS_TLSC_PLUS.1 SFR of the Security Target [ST].

- 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.

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: 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.

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

RACF:

- Do not use the RACF remote sharing facility (RRSF) in remote mode. If you use RRSF in local mode, ensure that command direction cannot be used by taking one of the following actions:

    - ensure that the RRFSFDATA class is not active;

    - define the profile DIRECT.* in the RRSFDATA class with UACC(NONE) and no users in the access list.

- Do not use multifactor authentication. You can disable the use of multifactor authentication by making the MFADEF class inactive.

Any client that is delivered with the product that executes with the user's privileges must be used with care, since the TSF cannot 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, for example, client programs for Telnet, TN3270, FTP, r-commands, and `ssh` 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 the Security Target [ST] or because they have not been included in the evaluated configuration. 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 the document [MLSGUIDE]:

- All Bulk Data Transfer (BDT) elements: BDT, BDT File-to-File, and BDT Systems Network Architecture (SNA) NJE.
- The DFS™ 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 document [MLSGUIDE].

9.3.2 Hardware installation and configuration

The TOE is one instance of z/OS running on an abstract machine as the sole operating system and exercising full control over this abstract machine. This abstract machine, which is not being part of the TOE, 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 (System z15);
- a certified version of IBM z/VM® executing in a logical partition provided by PR/SM on System z™ processors.

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

- all terminals supported by the TOE;
- all printers supported by the TOE;
- all storage devices and backup devices supported by the TOE;
- all Ethernet and token-ring network adapters supported by the TOE.

Note: The peripherals may be virtualized in the case of the TOE executing within a logical partition or z/VM. The logical partitioning software and z/VM software is part of the abstract machine and therefore part of the TOE environment. The logical partitioning software documentation as well as the z/VM documentation provides the required guidance on how to set up and configure the logical partitioning software or z/VM and how to define the logical peripheral devices so the TOE operates securely in the logical partitioning or z/VM environment.

Hardware configuration is further detailed in sect. 1.5.3.2 of the Security Target [ST].

10 Annex B – Evaluated configuration

The Target of Evaluation is “z/OS Version 2 Release 4”, developed by IBM Corp. The TOE is software only and is accompanied by guidance documentation. The items listed in Table 2 represent the TOE.

The z/OS V2R4 Common Criteria Evaluated Base package must be installed and configured according to the directions in section 9.3.1 as for the SW parts and directions in section 9.3.2 as for the HW parts.

11 Annex C –Test activities

This Annex describes the effort of both Developer and LVS in testing activities. For the assurance level EAL4, augmented with ALC_FLR.3, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 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" ([ZARCH]). The hardware platforms implementing this abstract machine are:

- IBM z15 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express7S cards.

Note that the above mentioned Crypto Express cards are not part of the TOE 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.

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 sect. 1.5.3.2 of the Security Target [ST].

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 4 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 behavior of the TOE, the Evaluators verified that all tests that might have been affected by any security-relevant change introduced later in the development cycle had been run on the evaluated configuration.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

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.

Functional Verification Tests (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. The BERD (Background Environment Random Driver) test driver submits the testcases as JES2 jobs. IBM's intention is to move more and more tests to this automated environment, which will ease the test effort required for the evaluations substantially. Starting with V1R9 a substantial number of tests has been ported to this environment. Additionally, most test teams ran their manual tests in the COMSEC test environment, which provides a complete test environment in the evaluated configuration of the TOE in the different modes of operation.

The test systems were running z/OS Version 2 Release 4 in the evaluated configuration. The Developer 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.

IBM's general test approach is defined in the process for Integrated Product Development (IPD) with Developer 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 Developer. 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 [ST] 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 has three cornerstones:

- The major internal security interface is the interface to RACF, which is tested exhaustively by the RACF test group.

- Components requiring Identification and Authentication or Access Control services call RACF. 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.

11.2.2 Test coverage

The Developer provided a mapping between the TSF of the Security Target [ST], the TSFI in the functional specification and the tests performed. The Evaluators 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.

11.2.3 Test results

The test results provided by the Developer 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 Evaluators verified that testing was performed on configurations conformant to the ST, with the exception of a number of patches, which has been accepted by the Evaluators after having examined their potential impact.

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

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

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The independent Evaluators testing followed the CEM guidance to test every security function, without striving for exhaustive testing.

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 [ST].

During dedicated sessions set up for the Evaluators to observe the testers running those tests, the Evaluators gained confidence in the Developers' approach for the test execution.

All Evaluators tests were run on the VICOM test system that had been set up by the Evaluators according to the specifications found in the guidance [MLSGUIDE]. One exception to this were additional patches, which the Developer recommends for the TOE, even though they were not part of the CC test installation. However, the Evaluators

provided a suitable justification for acceptance in the ATE activity report. Another configuration-related item that the Evaluators found was that the Developer COMSEC test machines did include components that are not part of the evaluation scope (e.g., components like Kerberos were installed on these systems). This also has been found to be acceptable, because they only increase the available interface, but do not affect the claimed security functionality.

11.3.2 Test coverage

For their own tests, the Evaluators decided to focus on different types of security functions of the TOE in order to provide independent verification of their correct operation:

- Identification and authentication: the Evaluators only devised some basic, testing of the identification and authentication functions for TSO/E (password, passphrase), and SSH, and console timeout enforcement. A new test was extended that tests the usability of user names longer than 8 characters, which has been a restriction for a very long time. In addition, while playing around with user management and TSO commands, the Evaluators initially found some seemingly unexpected behavior of non-RACF user management functions (UADS accounts), which they then further analyzed and tested.

- Communication security: the Evaluators chose to ensure that secure communications channel SSH implements all claimed ciphers, HMACs, and key exchange algorithms.

- RACF operator command authorization: verify default protection of RACF operator commands against use by unprivileged users.

- 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.

- Audit: the Evaluators tested that changing of the clock created corresponding audit records.

- 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 leftover information. All other self-protection features are properties that could not be easily be “challenged” by Evaluators tests.

11.3.3 Test results

All test cases devised by the Evaluators passed, i.e. the actual test results matched the expected results.

There were no failed tests that were caused by TOE behaviour different from the expected behaviour or violating requirements stated in the Security Target [ST].

11.4 Vulnerability analysis and penetration tests

11.4.1 Testing approach

The Evaluator analyzed the Security Target [ST], design documentation, and test results for potential vulnerabilities. In addition, the Evaluators performed a search on public sources for known or claimed potential vulnerabilities of the TOE or components of the TOE. Those searches did not immediately reveal any candidate for penetration testing. Also, the functionality newly claimed in the Security Target was too straightforward to implement to be a good candidate for penetration testing.

The Evaluators – also based on discussions they had with the IBM internal vulnerability assessment team – devised some penetration tests targeting functions that were not new for this version of the TOE.

11.4.2 Test coverage

11.4.2.1 Testing legacy system calls

A first set of penetration tests targeted legacy system calls that still exist in z/OS to keep compliance with even very old versions of the TOE. Some of those system calls are no longer used by newly developed programs since new functions provide a better support for application developers. The legacy system calls may therefore not have been modified since many years and due to their use mainly be legacy programs vulnerabilities within those system calls may have not been detected and reported in the last years.

One problem that some of those legacy system calls had in the past was their incomplete checking of a caller's access rights to memory locations whose addresses are passed to the system call. If such a memory location is fetch-protected for user programs, a system call function (which is not subject to the fetch protection) may reveal information about the content of the fetch-protected storage if it uses the memory without previously checking if the caller is allowed to read data from that memory location.

Instead a system call should – before accessing memory on behalf of the caller of the system call – check if the caller is allowed to access the memory location. The system call should return a memory access violation ABEND code when this is not the case.

Therefore, a program was developed that allowed to check a number of legacy system calls by passing in the memory address of a storage area previously identified as being fetch-protected for the calling program.

The penetration test was executed on 8 different legacy system calls. All of them returned the correct ABEND code for memory access violation.

11.4.2.2 Memory exhaustion attempt

A second penetration test was developed and executed that attempted to exhaust memory used internally by the TOE by having a program create as many specific system control blocks (in this case Task Control Blocks) as possible by creating new tasks in an infinite loop. The penetration test was executed and showed that the TOE is protected against such an attack and limits the number of tasks that can be created within an address space.

11.4.2.3 Password change test

A third penetration test was created testing for a potential race condition when a user is forced by the administrator to change his password. With the assumption that the temporary password assigned by the administrator could be known to an attacker, a penetration test was developed and executed where two persons (an intruder in addition to the legitimate user) logged into the TOE using the temporary password. If that had worked, both users would be requested to change the password. The test demonstrated that the TOE prohibited the second login thus allowing only one user with the same ID to authenticate to the TOE at a time, thereby prohibiting the attack.

11.4.3 Test results

In all cases the penetration tests ended with an error message showing that the TOE operated correctly.

In the case of the legacy SVC system calls tested for correctly checking the caller's access right to memory locations passed as parameter all SVCs tested ended with an ABEND code of 0C4 which indicates memory access violation detected.

In the case of the 'Rabbit' program creating tasks (and related task control blocks in system space) the TOE terminated the program with an error message stating that it detected a shortage in system space.

In the case of the password change test, the second login using a different login path was denied to change the password showing that the TOE correctly identified that a password change was already in progress.

11.4.4 Residual vulnerabilities

The Evaluators have also performed their vulnerability analysis based on the information provided in the Security Target [ST], the design documentation, the implementation representation and the user guidance. The Evaluators did not find any new vulnerability introduced by the new or modified functionality introduced with z/OS V2R4 that can be exploited in the operational environment. No vulnerability was reported in the public sources for vulnerabilities that the Evaluators checked (CVE, the z/OS specific RACF mailing list, general searches on the Internet).

It is worth highlighting that in the previous evaluation of the TOE z/OS V2R3 ([CR]) two residual vulnerabilities were detected (CVE-2018-0734, CVE-2018-0735). With the new implementation chosen by IBM for the affected cryptographic functions, these vulnerabilities have been removed in the current TOE.