Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ve.3.1 rel. 5

Certificato n. *(Certificate No.)*	08/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/05/2023/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	21 ottobre 2024
Nome e Versione del Prodotto *(Product Name and Version)*	IBM z/OS Version 2 Release 5
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistema Operativo
Conformità a PP *(PP Conformance)*	Protection Profile for General Purpose Operating Systems v.4.3
Funzionalità di sicurezza *(Conformance of Functionality)*	Funzionalità conformi a PP, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 21 ottobre 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) 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 Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM z/OS version 2 Release 5

OCSI/CERT/ATS/05/2023/RC

Version 1.0

21 October 2024

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute 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	21/10/2024

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AES	Advanced Encryption Standard
APAR	Authorized Program Analysis Report

APF	Authorized Program Facility
API	Application Programming Interface
APPC/MVS	Advanced Program-to-Program Communication / Multiple Virtual Storage
BCP	Base Control Program
BDT	Bulk Data Transfer
BSC	Binary Synchronous Communication
CBPDO	Custom-Built Product Delivery Option)
CLI	Command Line Interface
CM	Configuration Management
CPACF	Central Processor Assist for Cryptographic Function
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DES	Data Encryption Standard
DFS	Distributed File Service
DFSMS	Data Facility Storage Management Subsystem
DPCM	Decreto del Presidente del Consiglio dei Ministri
FTP	File Transfer Protocol
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICSF	Integrated Cryptographic Service Facility
ID	Identifier
IPSec	IP Security
JES	Job Entry System
LDAP	Lightweight Directory Access Protocol
NJE	Network Job Entry
OS	Operating System
PKCS	Public-Key Cryptography Standards

PR	Processor Resources
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
RRSF	RACF Remote Sharing Facility
RSA	Rivest-Shamir-Adleman
SAK	System Assurance Kernel
SHA	Secure Hash Algorithm
SM	System Manager
SMF	System Management Facilities
SNA	Systems Network Architecture
SQL	Structured Query Language
SSH	Secure SHell
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple DES
TLS	Transport Layer Security
XBM	Execution Batch Monitor
z/OSMF	z/OS Management Facility

4 References

4.1 Normative references and national Scheme documents

[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. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 5/23 - Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[ETR] Final Evaluation Technical Report IBM z/OS Version 2 Release 5, atsec information security s.r.l., version 2, 30 August 2024

[GPOSPP] Protection Profile for General Purpose Operating Systems Version 4.3, 27 September 2022

[MLSGUIDE] z/OS V2.5 Planning for Multilevel Security and the Common Criteria, code GA32-0891-50, 13 July 2024.

[SSHPKG] Functional Package for Secure Shell (SSH), v. 1.0, 13 May 2021

[ST] Security Target for z/OS v.2.17, 27 August 2024

[TLSPKG] Functional Package for Transport Layer Security (TLS) v.1.1, 1 March 2019

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

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

This certificate is recognised under SOGIS-MRA for all selected assurance components up to EAL4.

5.2 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] was 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 for all selected assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**IBM z/OS version 2 Release 5**", developed by International Business Machines (IBM) Corporation.

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 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, NIS5]. 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).

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 version 3.1 Revision 5 for the assurance components included in the PP General Purpose Operating System Protection Profile v.4.3 [GPOSPP], 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 named "IBM z/OS Version 2 Release 5" 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 also review 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 5
Security Target	Security Target for z/OS version 2.17, 27 Aug. 2024
Evaluation Assurance Level	Protection Profile Conformance
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	Protection Profile for General Purpose Operating Systems v.4.3, 27 Sept. 2022[1] [GPOSPP]
Evaluation starting date	May 30, 2023
Evaluation ending date	September 2, 2024

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 fulfilled and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description refer to the Security Target [ST].

The Target of Evaluation (TOE) is the z/OS operating system version 2 release 5 with the software components as described in Table 3, sect. 9.1.1 pag. 21.

Multiple users can use z/OS simultaneously to perform functions that require controlled, shared access to the information stored on the system. The TOE Security Functional Requirements are

[1] [GPOSPP] claims also conformance to Functional Package for Transport Layer Security (TLS) v.2.1 [TLSPACK] and to Functional Package for Secure Shell (SSH) v.1.0 [SSHPKG].

implemented by the following TOE Security Functions: identification and authentication, discretionary access control, auditing, security management, cryptographic support, Communications Security, TSF protection, confidentiality protection of datasets.

For a more detailed description of the TOE, please refer to sect. 1.5 ("TOE description") of the Security Target [ST].

7.3.1 TOE architecture

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 Processor Resources/System Manager (PR/SM) running on:
    - IBM z16 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express8S cards.
- a certified version of IBM z/VM executing in a logical partition provided by PR/SM on the above-mentioned z System z16 processor.

7.3.2 TOE security features

The primary security features of the TOE are:

- identification and authentication;
- discretionary access control;
- auditing;
- security management;
- cryptographic support;
- communication security;
- TSF protection;
- confidentiality protection of datasets.

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

7.3.2.1 Identification and Authentication

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

- an alphanumeric RACF user ID and a system-encrypted password or (for applications that support it) password phrase;
- an alphanumeric RACF user ID and a PassTicket, which is a cryptographically-generated password substitute encompassing the user ID, the requested application name, and the current date/time;
- an SSH key that is configured to be trusted by the user and that is presented to the SSH server during the authentication process.

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

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

The password quality can be tailored to the installation's policies using various parameters. When creating users, administrators are required to choose an initial password and optionally a password phrase, that must usually be changed by the user during the initial logon that uses the password/phrase. Administrators may configure a policy for the lockout of accounts.

7.3.2.2 Discretionary Access Control (DAC)

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.

7.3.2.3 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.

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

RACF always generates audit records for such events as unauthorized attempts to access the system or changes to the status of the RACF database. The security administrator, auditors, and other users with appropriate authorization can configure which additional optional security events are to be logged. RACF provides SMF records for all RACF-protected resources (either “traditional” or z/OS UNIX-based)

7.3.2.4 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 as well as general resource profiles.

7.3.2.5 Cryptographic support

The TOE provides cryptographic functions by the Integrated Cryptographic Services Facility (ICSF) subsystem. ICSF uses cryptographic hardware provided by the operational environment to provide and support cryptographic functions.

The TOE implements TLS Version 1.2 as well SSH version 2 for communication and remote access.

7.3.2.6 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. The confidentiality and integrity of network connections are assured by Transport Layer Security (TLS) encrypted communication for TCP/IP connections (Version 1.2). z/OS also supports the SSH v2 protocol and the ssh-daemon provided services of ssh (secure shell), scp (secure copy), and sftp (secure ftp).

7.3.2.7 TSF Protection

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

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

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

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

The TOE also provides the following mechanisms to protect its TSF:

- address space layout randomization (ASLR);
- stack buffer overflow protection;
- verification of integrity of the IPL process;
- trusted software updates using digital signatures.

7.3.2.8 Confidentiality protection of data sets

With z/OS confidentiality protection of data sets, users can encrypt data at rest without requiring application changes. z/OS data set encryption through RACF commands and policies allows the administrator to identify the data sets or groups of data sets that require encryption.

With data set encryption, the administrator is able to protect viewing the data in the clear. This is based on access to the key label that is associated with the data set and used by the access methods to encrypt and decrypt the data.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" 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 section 8.3 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims exact conformance to the Protection Profile for General Purpose Operating Systems v.4.3 [GPSOPP].

7.6 Functional and assurance requirements

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

All the SFRs included in the [GPOSPP] have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target claims exact conformance to the Protection Profile for General Purpose Operating Systems v.4.3 [GPOSPP], all the SFRs from such PP are included.

It is possible to 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 the same 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 [NIS5] 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 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 s.r.l.

The evaluation was completed on 2 September 2024 with the issuance by LVS of the Evaluation Technical Report v.2 [ETR] that has been approved by the Certification Body on 4 September 2024. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

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; there is a probability, however small, 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 regularly check 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 [ETR] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "IBM z/OS Version 2 Release 5" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance package defined in PP [GPOSPP], 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 package defined in [GPOSPP].

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
Basic functional specification	ADV_FSP.1	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
Implementation representation CM coverage	ALC_CMC.1	Pass
Authorisation controls	ALC_CMS.1	Pass
Test	**Class ATE**	Pass
Independent testing - sample	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.1	Pass

Table 1 Final verdicts for assurance requirements

8.2 Additional assurance activities

The Protection Profile for General Purpose Operating Systems v.4.3 [GPSOPP] includes additional assurance activities that are specific to the TOE technology type, and are required for conformance to the PP.

The Evaluators used for the PP assurance activities a notation similar to assurance components of existing CC assurance classes. The objective of these sub-activities is to determine whether the requirements of the assurance activities included in the PP are met.

Table 2 summarizes the final verdict of the PP assurance activities carried out by the LVS.

PP assurance activities		**Verdict**
ASE: Security Target evaluation	ASE_GPOSPP.1	Pass
	ASE_SSHPKG.1	Pass
	ASE_TLSPKG.1	Pass
AGD: Guidance documents	AGD_GPOSPP.1	Pass
	AGD_SSHPKG.1	Pass
	AGD_TLSPKG.1	Pass
ALC: Life cycle support	ALC_GPOSPP.1	Pass
ATE: Tests	ATE_GPOSPP.1	Pass
	ATE_SSHPKG.1	Pass
	ATE_TLSPKG.1	Pass
AVA: Vulnerability assessment	AVA_GPOSPP.1	Pass

Table 2 - Final verdicts for PP assurance activities

8.3 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “IBM z/OS Version 2 Release 5” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “Objectives for the Operational Environment” specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.2 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, “Annex A – Guidelines for the secure usage of the product” includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE.

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

9.1.1 Scope of TOE supply

The following Table 3 contains the elements provided with the TOE including software and guidance.

No	Type	Identifier	Release	Form of Delivery
z/OS Version 2 Release 5 (z/OS V2.5, program number1 5650-ZOS) Common Criteria Evaluated Base Package				
1	DOC	z/OS V2R5 Library Archive file name: zOSV2R5Library.zip SHA256 hashsum of the file: 52cfa67733c4e0d2c507e282d7f69f56cc13c7e7a0bbfe2a9507b86d7daaf056	V2R5	Electronic
		Download from https://www.ibm.com/docs/en/zos/2.5.0?topic=documentation-pdf-files-zos-250-library, "IBM z/OS 2.5 Adobe Indexed PDF Collection"		
2	DOC	Memo to Customers of z/OS V2.4 Common Criteria Evaluated Base	n/a	Hardcopy
3	DOC	[MLSGUIDE] z/OS V2.5 Planning for Multilevel Security and the Common Criteria File name: Planning_MLS_and_CC_zOS_V2R5.pdf Last updated: 2024-07-13	GA32-0891-50	Electronic
		SHA256 hashsum of the document: abb7bb5c4c86667a7363868bb966eb2ec005d9a0b1178b4a9363111cab2fdc9d		
Additional Media				
4	SW	PTFs for the following APARs (required): • Documentation APAR OA64593 • Documentation APAR OA66552 • APAR OA66005 and its corresponding PTF These PTFs are to be obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)	n/a	Electronic

Table 3 - TOE Deliverables

9.1.2 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.

Internet orders

Order content is staged to an IBM download server and *Shopz* (www.ibm.com/software/shopzseries/ShopzSeries_public.wss) generates a customized download page for each order. The download page includes links for order content and instructions.

The integrity of Internet orders is ensured by SHA-1 hashing algorithm and verification is used if the digital signature is not verified. CBPDO (Custom-Built Product Delivery Option) and z/OSMF (z/OS Management Facility) ServerPac order packages are signed by IBM and the digital signature can be optionally verified. Furthermore, a unique client and server public/private key pair is created. CBPDO and z/OSMF ServerPac order packages are signed by IBM and the digital signature can be optionally verified.

Under subsection "Security of your Internet order", the plan installation guide describes that the internet delivery method uses a combination of standard authentication and data integrity approaches to provide security for information about the order and to ensure the integrity of the contents of the order using *Shopz* user ID and password.

Hashing algorithms are used for both download methods (directly to z/OS and to a workstation as an intermediate node). For downloads directly to z/OS, SMP/E (System Modification Program/Extended) ensures the data integrity of the package through its assignment of a hash value and digital signature during packaging of the order and required verification of that hash value and optional verification of the digital signature upon download. SMP/E uses the ICSF One-Way Hash Generate callable service to perform the verification.

When using Secure FTP (FTPS) or HTTP Secure (HTTPS) to download the order directly to the z/OS host system, the package is encrypted during transmission. When using Download Director to download the order to a workstation as an intermediate node, the package is encrypted during transmission.

Furthermore, in subsection "Network security", the guide explains that before downloading the order, the customer must understand the network security environment.

- If the customer is planning to download directly to z/OS, he must be familiar with the security and networking information that is required to navigate his enterprise's firewall or proxy server from z/OS (for a ServerPac or for CBPDO).

  Server information defines the IBM download server where the order resides. The server information specifies the IP address or hostname of the IBM download server, and the User ID and password information to access the IBM download server.

- If the customer is downloading the order to a workstation and he plans to use SMP/E RECEIVE FROMNETWORK to transfer the order to z/OS, he must update the server information to reflect the workstation's FTP server information.

  Client information describes the IP address or host name of the firewall or proxy server, IP port, User ID and password, Account information, Firewall-specific or proxy server commands, Signature keyring if the customer is verifying the package signature.

ServerPac uses the One-Way Hash Generate callable service to verify the SHA-1 hash value associated with the package. To receive the order by using FTPS, ICSF must be configured and active. To receive the order by using HTTPS, the SMP/E Java application class must be available.

Finally, the “z/OS Planning for Installation” in subsection "Security for signed software packages" explains that z/OS SMP/E and z/OSMF Software Management provide the ability to digitally sign and verify the signature of GIMZIP software packages that are delivered both electronically and physically, on all supported z/OS releases. This capability ensures that a software package is not modified since it was created and is signed by the expected provider.

A signed product package contains an SHA-256 hash for each file, and an SHA-256 with RSA signature for the package.

Both z/OSMF ServerPac and CBPDO order packages are signed by IBM. Observe the following considerations:

- IBM signs z/OSMF ServerPac portable software instance packages, including all electronic and DVD packages for all SRELs.
- IBM signs CBPDO order packages, including all electronic and DVD packages for all SRELs.

In addition, the TOE delivery process implies a very special ordering process, indeed the TOE is not a standard off-the-shelf-product but requires specific hardware to be run on as stated in 1.5.3.1 "Software Configuration" of the [ST], which is only available from IBM and already involves a business relationship.

Electronic delivery of the guidance is provided through the IBM web site at https://www.ibm.com/docs/en/zos/2.5.0?topic=documentation-pdf-files-zos-250-library. Users can retrieve the whole guidance package for the TOE (see item #2 in above) by clicking the link "IBM z/OS 2.5 Adobe Indexed PDF Collection". 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 window to verify the IBM certificate. The resulting ZIP archive named zOSV2R5Library.zip will also contain the manual (see item #3 in Table 3 above), which contains further instructions on how to set up the TOE in its evaluated configuration.

9.2 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage should be done by following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the documents provided by IBM, as described in section 9.1.2, contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

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

The z/OS V2R5 Common Criteria Evaluated Base package must be installed according to the directions delivered with the media and configured according to the instructions in [MLSGUIDE] chapter 7. Also, all required PTFs as listed as item #4 in Table 3 above must be installed.

The installation can choose not to use any of the elements delivered within the ServerPac.

However, user must install, configure, and use at least the RACF component of the Security Server optional feature and the ICSF component of Cryptographic Services.

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.
- Adding user own local checks to the Health Checker for z/OS because those checks run authorized. If there is the need to add user own checks, add them as unauthorized remote checks.
- Using the Authorized Caller Table (ICHAUTAB) in RACF to allow unauthorized programs to issue RACROUTE REQUEST=VERIFY (RACINIT) or RACROUTE REQUEST=LIST (RACLIST).

The SSH daemon *sshd* is part of the TOE, if used:

- Must be configured to use protocol version 2 and at least one of the AES-based cipher suites stated in the [ST].
- 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. Host-based and public-key based user authentication with the keys stored elsewhere cannot be used in the evaluated configuration.
- It must be configured with the ForwardAgent option set to OFF, which is the default.
- It must be configured with the AuthorizedKeysCommand and AuthorizedPrincipalsCommand settings disabled.

TLS:

- TLS (Transport Layer Security) processing, if used, must use TLS V1.2 protocol. TLS (Transport Layer Security), if used, must use one of the cipher suites listed in the FCS_TLSS_EXT.1 and FCS_TLSC_EXT.1 SFRs of the 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;
- Any application that uses TLS with client or server authentication must be configured for revocation checking through OCSP responses.

RACF:

- Do not use the RACF remote sharing facility (RRSF) in remote mode. If there is the need to 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. User 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 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, 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 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 [MLSGUIDE]:

- Apache Server
- BCPii
- 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
- IPsec
- JES3
- Kerberos
- LDAP
- NFS
- PKI Services
- SUDO

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.
- The multi-level security environment.
- JES2 NJE communication via TCP/IP. JES2 NJE must use SNA or BSC in the certified configuration.
- JES2 Execution Batch Monitor (XBM) facility.

10 Annex B – Evaluated configuration

The Target of Evaluation is "z/OS Version 2 Release 5", developed by IBM Corp. The TOE is software only and is accompanied by guidance documentation. The items listed in Table 3 represent the TOE.

The TOE name and version number uniquely identify the TOE and its components, which constitute the evaluated configuration of the TOE verified by the evaluator at the time they perform the tests and to which the evaluation results apply.

10.1 TOE operational environment

The following assumptions about the technical environment in which the TOE is intended to be used are made.

The TOE is running a logical partition provided by PR/SM or a certified version of z/VM on one of the following z System™ processors:

- IBM z16 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express8S (CEX8) cards.

The following peripherals can be used with the TOE.

- All terminals that are supported by the TOE.
- Printers:
  - any printer that is supported by the TOE.
- All storage devices and backup devices supported by the TOE, such as:
  - direct access storage devices (DASDs), except RVA devices;
  - tape drives (including encrypting tape drives, though this evaluation has not specifically examined those cryptographic functions).
- All Ethernet and token-ring network adapters that are supported by the TOE.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The test system were running z/OS Version 2 Release 5 which the evaluator found to be consistent with the Evaluated Configuration in Annex B and the Security Target [ST].

All testing activities have been carried out remotely from the LVS premises having full and exclusive control on the test machine.

11.2 Functional tests performed by the Developer

No developer test assessment required at this assurance level.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

The Security Target [ST] claims exact conformance to the PP [GPOSPP], which defines test cases mapped to SFRs. The Evaluators performed both automated and manual test cases defined by evaluation activities in [GPOSPP] with the addition of Technical Decisions listed in [ST] section 2.1 "Protection Profile Tailoring and Additions", to fulfil the required tests, thereby also fulfilling the requirements for ATE_IND.1.

11.3.2 Test results

All Developer’s tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the test environment and TOE already used for the functional test activities, verifying that the TOE and the test environment were properly configured.

Since an attack requires an attack surface, the Evaluators decided to examine if the TOE exposes such interfaces, i.e., open ports. Port scans were performed against the TOE interfaces that are accessible to a potential attacker. The Evaluators examined all potential interfaces (IPv4 and IPv6 TCP and UDP ports of the TOE).

Evaluator, based on search result, compiled a table of potentially applicable vulnerabilities: based on the analysis, the evaluator determined there are no potential vulnerabilities in the TOE.

The Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operating environment. No exploitable or residual vulnerabilities have been identified.