Agenzia per la Cybersicurezza Nazionale

OCSI

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) ver.3.1 rel. 5

Certificato n. *(Certificate No.)*	07/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/15/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	9 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	IBM z/VM Version 7.4 with RSU1 and CP service level 0002 for VPP
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistemi Operativi (Operating Systems)
Conformità a PP *(PP Conformance)*	Protection Profile for Virtualization. Ver.1.1, PP-Module for Server Virtualization Systems. Ver. 1.1, PP-Configuration for Virtualization and Server Virtualization Systems. Version1.0, Functional Package for Transport Layer Security (TLS), CC Parte 3 estesa
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, 9 febbraio 2026

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/VM Version 7.4 with RSU1 and CP service level 0002 for VPP

OCSI/CERT/ATS/15/2024/RC

Version 1.0

9 February 2026

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	09/02/2026

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

APAR	Authorized Program Analysis Report
API	Application Programming Interface

CMS	Conversational Monitor System
CP	Control Program
DAC	Discretionary Access Control
I/O	Input/Output
ID	Identifier
IPL	Initial Program Load
IUCV	Inter User Communication Vehicle
LGR	Live Guest Relocation
LPAR	Logical Partition
LS	Labeled Security
MAC	Mandatory Access Control
MFA	Multi-factor Authentication
OSPP	Operating System Protection Profile
PDF	Portable Document Format
PR/SM	Processor Resource/System Manager
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
RSU	Recommended Service Upgrade
SDF	Software Delivery and Fulfillment
SIE	Start Interpretive Execution
SSI	Single System Image
SSL	Secure Sockets Layer
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VIRT	Virtualization

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. 3/23 - Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[CCGUIDE] IBM Corporation, z/VM 7.4 Secure Configuration Guide, v SC24-6323-08 (January 2026), Common Criteria NIAP VPP 1.1 Certification.

[ETRv1] Final Evaluation Technical Report zVM Version 7 Release 4 for (OCSI-CERT-ATS-15-2024), v.1.0 atsec information security s.r.l., 28th November 2025.

[ETRv2] Final Evaluation Technical Report zVM Version 7 Release 4 for (OCSI-CERT-ATS-15-2024), v.2.0 atsec information security s.r.l., 9 February 2026.

[INST_GUIDE] z/VM 7.4 Installation Guide, IBM Corporation v. GC24-6292-05, July 2025.

[MOD_SV] PP-Module for Server Virtualization Systems. Version 1.1, 14th June 2021.

[OPE] "z/VM 7.4 2025 July PDF collection", v. 7.4 - 2025 Q2 NFA, July 2025.

[PKG_TLS] Functional Package for Transport Layer Security (TLS). Version 1.1, 1st March 2019.

[ST] IBM z/VM Version 7.4 with RSU1 and CP service level 0002 for VPP Security Target – v1.0 – 19 January 2026.

[SVCONFIG] PP-Configuration for Virtualization and Server Virtualization Systems. Version1.0, 4th June 2021.

[VPP] Protection Profile for Virtualization. Version 1.1, 14th June 2021.

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 claimed 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 8 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 claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**IBM z/VM Version 7.4 with RSU1 and CP service level 0002 for VPP**", also referred to in the following as (IBM) z/VM Version 7 Release 4, z/VM V7R4 or z/VM, developed by International Business Machines (IBM) Corporation.

The TOE is a virtual machine hypervisor for IBM Z servers onto which to deploy mission critical virtual servers

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 provided for the evaluation assurance level defined by the SARs included in the PP [VPP] 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/VM Version 7.4 with RSU1 and CP service level 0002 for VPP" 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/VM Version 7.4 with RSU1 and CP service level 0002 for VPP
Security Target	IBM z/VM Version 7.4 with RSU1 and CP service level 0002 for VPP Security Target – v1.0 – 19 January 2026 [ST]
Evaluation Assurance Level	PP conformant with the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1 ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	[VPP]: Protection Profile for Virtualization. Version 1.1 [MOD_SV]: PP-Module for Server Virtualization Systems. Version 1.1 [SVCONFIG]: PP-Configuration for Virtualization and Server Virtualization Systems. Version1.0 [PKG_TLS]: Functional Package for Transport Layer Security (TLS). Version 1.1.
Evaluation starting date	June 26th, 2024
Evaluation ending date	November 28th, 2025

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 TOE is the z/VM Version 7 Release 4 clustered as up to eight cooperating instances of z/VM within a Single System Image (SSI).

z/VM is a virtual machine hypervisor for IBM Z mainframe servers onto which to deploy mission-critical virtual servers. A single z System server can host one z/VM instance per logical partition (LPAR), and each instance of z/VM can host tens to hundreds of virtual servers. Multiple instances of z/VM can be connected to form a networked system called a "collection".

The communication aspects within z/VM used for these connections are also part of the evaluation. External communication links can be protected against loss of confidentiality and integrity by cryptographic protection mechanisms.

z/VM offers multi-system clustering technology allowing between one and eight z/VM instances in a SSI cluster. New instances of z/VM can be added to the cluster topology at runtime. Support for Live Guest Relocation (LGR) allows the movement of Linux virtual servers without disruption to the operation. The z/VM systems are aware of each other and can take advantage of their combined resources. LGR enables clients to avoid loss of service due to planned outages by relocating guests from a system requiring maintenance to a system that remains active during the maintenance period.

Note, the functionality of SSI is not covered by security claims in the ST [ST].

Due to the functionality of virtual machine monitor, the protection profile for virtualization [VPP] is used as a basis for the [ST]. z/VM meets all of the requirements of the VPP. In addition, z/VM provides extensive administration capabilities and thus meeting the requirement from the protection profile for virtualization extended package for server virtualization [MOD_SV].

z/VM provides identification and authentication of users using different authentication mechanisms, both discretionary and mandatory access control to a large number of different objects, separation of virtual machines, a configurable audit functionality, sophisticated security management functions, preparation of objects for reuse and functionality used internally to protect z/VM from interference and tampering by untrusted users or subjects tampering by untrusted user or subject.

For a detailed description of the TOE, refer to sections 1.3 and 1.4 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is the z/VM hypervisor product that is part of an SSI cluster formed by one or more z/VM instances with the software components as described in section 1.5.4 of the Security Target [ST].

z/VM is an operating system designed to host other operating systems, each in its own virtual machine. Multiple virtual machines can run concurrently to perform a variety of functions requiring controlled, separated access to the information stored on the system. The TOE provides a virtual machine for each logged in user, separating the execution domain of each user from other users as defined in the virtual machine definitions stored in the system directory. In addition, the system directory contains access control information for privileged functions, such as use of certain options of the processor's DIAGNOSE instruction. In addition to the system directory, the RACF security server is employed to mediate access to resources and privileged functions.

The TOE is seen as one instance of an z/VM SSI cluster comprising of one through eight individual z/VM systems. These individual z/VM systems each execute on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over this abstract machine regardless which software runs inside of virtual machines. These abstract machines are provided by logical partitions of IBM Z server.

The LPAR itself is not part of the TOE but belongs to the TOE environment.

It is to be noted that although a z/VM instance can be run within a z/VM instance, the evaluated configuration is restricted to one z/VM instance running directly within an LPAR. A z/VM instance running within a virtual machine is allowed, but such "second level" z/VM instances are not part of the evaluated configuration as some security functionality is implemented differently, in particular with respect to the usage of the processor's Start Interpretive Execution (SIE) instruction.

The z/VM SSI feature enables up to eight z/VM systems to be configured as members of an SSI cluster, sharing different resources.

All z/VM member instances of one SSI cluster hold distinct RACF database. Each z/VM member instance must execute its own instance of RACF accessing the dedicated RACF database. **Sharing of the RACF database between z/VM members is strictly prohibited in the evaluated configuration**.

The platforms selected for the evaluation consist of IBM products, which are available when the evaluation has been completed and will remain available for some period of time afterwards. Even if withdrawn from general marketing, the product may be obtained by special request to IBM.

The TOE security functions (TSFs) are provided by the z/VM operating system kernel (called the Control Program - CP) and by an application called RACF that runs within a specially-privileged virtual machine. In addition to providing user authentication, access control, and audit services to CP, RACF can provide the same services to other authorized virtual machines. z/VM provides management functions that allow configuring the TSF and tailor them to the customer's needs.

Some elements have been included in the TOE which do not provide security functions, but run in authorized mode and could therefore, if misbehaved, compromise the TOE. Since these elements are substantial for the operation of many customer environments, they are included as trusted applications within the TOE.

z/VM also provides the administration capabilities that cover the virtualization extended package for server virtualization [MOD_SV].

7.3.1.1 Major software components of the TOE

The TOE consists of up to eight z/VM instances each defined by the following major components: the CMS for operating RACF and TCP/IP, the z/VM Control Program (CP), the Security Manager RACF, and the TCP/IP for z/VM component.

The z/VM CP is primarily a real-machine resource manager. CP provides each user with an individual working environment known as a virtual machine. Each virtual machine is a functional equivalent of a real system, sharing the real processor instructions and its functionality, storage, console, and I/O device resources. CP provides connectivity support that allows application programs running within virtual machines to exchange information with each other and to access resources residing on the same z/VM system or on different z/VM systems.

In order to create and maintain these rules (virtual machine definitions), additional management software is employed, that runs outside the CP, but is part of the TOE. Hence, each component of the management software runs within a virtual machine. The following list illustrates, which functionality runs within virtual machines:

- **CMS (Conversational Monitor System)**: a single-user general-purpose operating system that is employed to run the RACF and TCP/IP applications;
- **RACF server**: provides authentication, authorization, and audit services to CP and other authorized virtual machines that run applications on CMS. It runs within a virtual machine maintained by CP and communicates with CP through a tightly controlled well-defined interface;
- **TCP/IP server**: provides traditional IP-based communications services. It is not part of CP, but runs within a virtual machine. Embedded within the TCP/IP stack is the Telnet service that enables users to access their virtual machine consoles ("log on") from the IP network. In particular, this Telnet service receives console traffic from the network, removes the telnet or TN3270 protocol wrappers, and then forwards it to CP using a special form of the DIAGNOSE processor instruction. CP generates a virtual console session as a memory object. All outgoing information is sent from the CP back to the Telnet service, which encapsulates the information in the Telnet or TN3270E protocol and sends it back to the client. The TCP/IP server also provides TLS allowing the establishment of a cryptographically secured channel

7.3.2 TOE security features

Assumptions, threats and security objectives are defined in section 3 and 4 of the Security Target [ST].

The major security features of the TOE are summarised in the following sections.

7.3.2.1 TOE Security Policies

The security policy enforced is defined by the selected set of Security Functional Requirements (SFR) and implemented by the TOE. The TOE implements policies pertaining to the following security functional classes: Security Audit (FAU), Cryptographic Support (FCS), User Data Protection (FDP), Identification and Authentication (FIA), Security Management (FMT), Protection of the TSF (FPT), TOE Access (FTA), and Trusted Path/Channels (FTP).

7.3.2.2 Security objectives for the operational environment

All security objectives for the Operational Environment in the [ST] are reproduced from the [VPP] and [MOD_SV]:

- **OE.CONFIG:** *TOE administrators will configure the Virtualization System correctly to create the intended security policy.*
- **OE.PHYSICAL:** *Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.*
- **OE.TRUSTED_ADMIN:** *TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.*
- **OE.NON_MALICIOUS_USER:** *Users are trusted to not be willfully negligent or hostile and use the VS in compliance with the applied enterprise security policy and guidance.*

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

The most significant aspects are summarized below:

- **Identification and Authentication:** the TOE provides identification and authentication of users by the means of an alphanumeric user ID and a system-encrypted password/passphrase. The following parts of the TOE perform identification and authentication independently:
  - Control Program;
  - RACF.

  For supporting identification and authentication, the TOE employs RACF managing resource profiles and user profiles.
- **Discretionary Access Control (DAC):** for implementation of extended DAC rules, the TOE component RACF provides the capability and flexibility as required by the evaluation compared to the usage of the system. Basically, a user's authority to access a resource while operating in a RACF-protected system at any time is determined by a combination of these factors:
  - user's identity and group membership;
  - user's attributes including group-level attributes;
  - user's group authorities;
  - security classification of the user and the resource profile;
  - access authority specified in the resource profile.
- **Separation of virtual machines:** Operating system failures that occur in virtual machines do not normally affect the z/VM operating system running on the real processor. If the error is isolated to a virtual machine, only that virtual machine fails, and the user can re-IPL (Initial Program Load) without affecting the testing and production work running in other virtual machines.

  Supported by the underlying processor, the TOE restricts results of software failures (such as program checks) occurring in a virtual machine to this machine, thus not affecting other virtual machines or the CP.

  Failures of CP that cannot be isolated to a particular virtual machine result in the abnormal termination ("abend") of the Control Program. In the event of such an abend, the system will re-initialize itself, if possible. Special abend code numbers are used to identify the specific reason for the abend.
- **Audit:** The TOE provides an audit 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 the resource. The audit records generated by RACF are collected into files residing on disks that are protected from unauthorized modification or deletion by the DAC and (in Labeled Security Mode) MAC mechanism.
- **Object Reuse:** The TOE provides a facility clearing protected objects and storage previously used by virtual machines or the TOE itself prior to reassignment to other virtual machines or the TOE. This ensures confidentiality of data maintained either by the TOE or by virtual machines.

Storage devices and their derivatives (such as minidisks or temporary disks) are to be cleared manually by the administrator in accordance with the organizational policies. There is additional software support by the IBM Directory Maintenance Facility (DirMaint), which however is not part of this evaluation.

- **Security Management:** The TOE provides a set of commands and options to adequately manage the security functions of the TOE. The TOE recognizes several roles that are able to perform the different management tasks related to the TOE's security:
    - general security options are managed by security administrators;
    - management of users and their security attributes is performed by security administrators. Management of groups can be delegated to group security administrators;
    - management of virtual machine definitions is performed by security administrators;
    - users are allowed to change their own password, their default group, and their user name;
    - users may choose their security label from the range defined in their profile at login time in Labeled Security mode;
    - auditors manage the parameters of the audit system (e.g. list of audited events and can analyse the audit trail.
- **TSF Protection:** The TOE control program enforces integrity of its own domain. No virtual machine can access TOE resources without appropriate authorization. This prevents tampering with TOE resources by untrusted subjects.

  Supportive to this functionality are hardware implemented facilities, namely the Interpretive Execution Facility (SIE instruction). Therefore, the hardware and firmware components providing the abstract machine for the TOE are required to be physically protected from unauthorized access.
- **Cryptographic Support:** The TOE provides cryptographically protected communication links, based on the TLS version 1.2 protocol suite.

  The TOE supports the generation of strong random numbers to facilitate the generation of secure, unpredictable keys.

For a detaliled description of the TOE security functions refer to sections 1.4, 1.5 and 7 of Security Target [ST].

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 of 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 9 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims *exact conformance* to the following:

- [VPP]: Protection Profile for Virtualization. Version 1.1;
- [MOD_SV]: PP-Module for Server Virtualization Systems. Version 1.1;
- [SVCONFIG]: PP-Configuration for Virtualization and Server Virtualization Systems. Version 1.0;
- [PKG_TLS]: Functional Package for Transport Layer Security (TLS). Version 1.1.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived by extension from CC Part 3 [CC3]. This includes *ALC_TSU_EXT.1.1 - Timely Security Updates*, as defined in [VPP].

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

It is possible to refer to the Security Target [ST] for the description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFRs) 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]. In addition, all specific assurance activities required by the Protection Profile [VPP] have been performed.

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 November 28th, 2025 with the issuance by LVS of the Evaluation Technical Report v.1.0 [ETRv1] that has been approved by the Certification Body on 22 December 2025. The LVS has then issued a Final Evaluation Technical Report [ETRv2] with some editorial updates. Finally, 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 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 v.1.0 [ETRv1] 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/VM Version 7.4 with RSU1 and CP service level 0002 for VPP” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level defined by the SARs included in the PP [VPP], 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 components reported in defined by the SARs included in the PP [VPP] (In *Italics* are reported the extended assurance components).

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
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Timely Security Updates	*ALC_TSU_EXT.1*	*Pass*
Test	**Class ATE**	Pass
Independent testing - Conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability survey	AVA_VAN.1	Pass

Table 1 Final verdicts for assurance requirements

8.2 Additional assurance activities

The Protection Profile for Virtualization [VPP] includes additional assurance activities specific to the TOE technology type, and are required for exact 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. summarizes the final verdict of the PP assurance activities carried out by the LVS

PP assurance activities[1]		**Verdict**
ASE: Security Target evaluation	ASE_BVPP.1	Pass
	ASE_SVPPM.1	Pass
	ASE_TLSPKG.1	Pass
AGD: Guidance documents	AGD_BVPP.1	Pass
	AGD _SVPPM.1	Pass
	AGD _TLSPKG.1	Pass
ALC: Life cycle support	ALC_BVPP.1	Pass
ATE: Test	ATE_BVPP.1	Pass
	ATE _SVPPM.1	Pass
	ATE _TLSPKG.1	Pass
AVA: Vulnerability assessment	AVA_BVPP.1	Pass

Table 2 – Final verdict for additional 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/VM Version 7.4 with RSU1 and CP service level 0002 for VPP” 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.

[1] Activities with the _BVPP, _SVPPM, _TSLPKG, extension were entered by the lab to clearly organize the activities from the VPP's “Assurance Activities”, and related to activities for verification SFRs from PP-Module for Server Virtualization Systems [MOD_SV] and Functional Package for TSL [PKG_TLS] respectively.

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 [CCGUIDE].

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 3contains the item that comprise the different elements of the TOE.

No	Type	Identifier	Release/Version	Form of Delivery
1	SW	z/VM version 7 release 4, program n. 5741-A10	n/a	Digital copy via https://www.vm.ibm.com/service/getshopz.html
2	DOC	Program Directory for z/VM version 7 release 4	GI13-4358-03	Digital copy via https://www.vm.ibm.com/progdir/
3	DOC	Program Directory for RACF Security Server for z/VM function level 740	GI13-4364-03	
4	DOC	Program Directory for TCP/IP for z/VM Level 740	GI13-4360-03	
5	DOC	z/VM 7.4 Installation Guide	GC24-6292-05	Digital copy via https://www.vm.ibm.com/security/pubs.html
6	DOC	z/VM 7.4 Secure Configuration Guide	SC24-6323-08	
7	ZIP	z/VM 7.4 Common Criteria Collection Kit (2025 July PDF collection)	7.4 - 2025 2Q NFA	

No	Type	Identifier	Release/Version	Form of Delivery
8	SW	RSU1 (7401RSU) z/VM RSU7401, September 20 2024, RSU packaged with z/VM 7.4 installation media.	7401RSU	Digital copy via https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss
9	SW	PTF UM90474 for APAR VM66795 Level 0002, September 20 2024 z/VM 7.4 CP SECURITY APAR - Feature 00 Fix 02	UM90474	

Table 3 - TOE Deliverables

9.1.2 Delivery procedure

Customer can use the https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss portal to file an order for the TOE. In order to be able to place an order, the customer must provide an IBM customer ID. In case the customer needs assistance, they may contact an IBM sales representative who will then support the customer with filling out an order form.

9.1.2.1 Delivery to the customer

Incoming orders for z/VM are processed by an SDF (Software Delivery and Fulfillment) Production center. The z/VM image ordered is packed to an appropriate digital archive. The customer can download his order from the ShopZ page "My orders". Within this page the id assigned to the order is shown, and the RSU1 materials is included with the product package to be downloaded through HTTPS protocol into the customer workstation.

9.1.2.2 Customer's TOE verification

Once the download is completed the customer will be able to verify that the materials match the order by reviewing the content provided in the "Packing list for Order" in the ShopZ "My orders" page provided as part of the delivery and by cross checking the part numbers labeled on the downloaded material. The Installation Instructions included in the delivery of the order contain the SHA fingerprint of the installation media to be compared to the downloaded installation media. For service orders, such as PTF UM90474, the GIMPAF.xml is a cover letter included in the delivery of the order, and it contains the list of the files that make up the delivery with their respective SHA fingerprint. The cover letter has a self-contained SHA fingerprint. During transfer of the data through ShopZ using GetShopz, the fingerprint for each file is computed and compared with the stated fingerprint in the cover letter.

9.1.3 Identification of the TOE by the user

During the order process for the TOE, the customer needs to explicitly order the CC-certified version of z/VM Version 7 Release 4. This already ensures that the product delivered to the customer actually is the TOE containing all required components.

The administrator after installation of the product according to the Secure Configuration Guide also is able to verify the version of the TOE by issuing the command

QUERY CPLEVEL,

which will result in displaying the version string

z/VM Version 7 Release 4.0, service level 0002 (64-bit)

In addition, the administrator is asked to verify the list of installed PTFs against the list of PTFs required as stated in the ST. In order to do so, the administrator may issue the commands

- VMFSIM QUERY 7VMCPR40 SRVAPPS * TDATA :PTF
- VMFSIM QUERY 7VMRAC40 SRVAPPS * TDATA :PTF
- VMFSIM QUERY 7VMTCP40 SRVAPPS * TDATA :PTF

and should be able to verify the presence of the following PTFs in the output received.

For CP, the following PTFs should be reported:

- UM90474
- RSU1

For RACF and TCPIP, no PTFs should be reported.

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 [INST_GUIDE], [CONFIG] and [OPE] 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].

10 Annex B – Evaluated configuration

The Target of Evaluation is "IBM z/VM Version 7 Release 4 with RSU1 and CP service level 0002 for VPP", developed by IBM Corporation. Table 3 enlists the components of the TOE.

The TOE is accompanied by guidance documentation [CCGUIDE] and [INST_GUIDE]. 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 Evaluators at the time they perform the tests and to which the evaluation results apply.

10.1 TOE operational environment

The assumptions about the operational environment in which the TOE is intended to be used are reported in section 4.2 of [ST].

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 systems were running IBM z/VM Version 7 Release 4 in the evaluated configuration.

All testing activities have been carried out remotely from the LVS premises having full and exclusive control on the test machine as per [NIS5].

11.2 Functional tests performed by the Developer

No developer tests assessment is required by the assurance requirements described in [ST] and om [VPP].

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

The Evaluators performed tests following the CEM approach to test every security function, without striving for exhaustive testing: Evaluators devised a test strategy for the tests they intended to run the set of tests they were developing themselves. The Evaluators performed testing remotely by connecting to the test environment using IBM hardened laptops. The developer set up the test environment with the actual TOE model in Poughkeepsie, New York (USA). The testing was performed between October and November 2025. The Evaluators developed automated, partially automated and manual test procedures: The TOE claims exact conformance to the [VPP] and [MOD_SV]. The Evaluators, for each SFR declared in the [ST], has performed all tests required by the [VPP] and the selected packages ([MOD_SV] and [PKG_TLS]) with the addition of Technical Decisions listed in [ST], section 2 "CC Conformance Claim".

11.3.2 Test result

All test cases devised by the Evaluators were run 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.

The Evaluators analysed 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. The Evaluators also performed

- fuzzing penetration testing activities against zVM Guest CP and System SSL;
- testing for bypassing of the TELNET server.

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