



Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione



Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 10/22

(Certification No.)

Prodotto: IBM z/VM Version 7 Release 2 for VPP

(Product)

Sviluppato da: IBM Corporation

(Developed by)

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

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

Conforme a: Protection Profile for Virtualization, v1.0

(Conformant to)

(ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.1, 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)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 10 giugno 2022



This page is intentionally left blank



Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione



Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM z/VM Version 7 Release 2 for VPP

OCSI/CERT/ATS/04/2021/RC

Version 1.0

10 June 2022

Courtesy translation

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

1 Document revisions

| Version | Author | Information | Date |
|---------|--------|-------------|------------|
| 1.0 | OCSI | First issue | 10/06/2022 |
| | | | |

2 Table of contents

| | | |
|-------|--|----|
| 1 | Document revisions | 5 |
| 2 | Table of contents | 6 |
| 3 | Acronyms | 8 |
| 4 | References..... | 10 |
| 4.1 | Criteria and regulations | 10 |
| 4.2 | Technical documents | 11 |
| 5 | Recognition of the certificate..... | 12 |
| 5.1 | International recognition of CC certificates (CCRA)..... | 12 |
| 6 | Statement of certification..... | 13 |
| 7 | Summary of the evaluation | 14 |
| 7.1 | Introduction..... | 14 |
| 7.2 | Executive summary | 14 |
| 7.3 | Evaluated product | 15 |
| 7.3.1 | TOE architecture | 16 |
| 7.3.2 | TOE security features..... | 18 |
| 7.4 | Documentation | 20 |
| 7.5 | Protection Profile conformance claims | 20 |
| 7.6 | Functional and assurance requirements | 20 |
| 7.7 | Evaluation conduct..... | 21 |
| 7.8 | General considerations about the certification validity..... | 21 |
| 8 | Evaluation outcome..... | 22 |
| 8.1 | Evaluation results | 22 |
| 8.2 | Additional assurance activities..... | 23 |
| 8.3 | Recommendations | 23 |
| 9 | Annex A – Guidelines for the secure usage of the product..... | 25 |
| 9.1 | TOE delivery..... | 25 |
| 9.2 | Identification of the TOE..... | 26 |
| 9.3 | Installation, initialization and secure usage of the TOE | 27 |
| 10 | Annex B – Evaluated configuration..... | 28 |
| 11 | Annex C – Test activity..... | 29 |

| | | |
|------|--|----|
| 11.1 | Test configuration..... | 29 |
| 11.2 | Functional and independent tests performed by the Evaluators | 29 |
| 11.3 | Vulnerability analysis and penetration tests | 30 |

3 Acronyms

| | |
|--------------|---|
| APAR | Authorized Program Analysis Report |
| CAVS | Cryptographic Algorithm Validation System |
| CC | Common Criteria |
| CCRA | Common Criteria Recognition Arrangement |
| CEM | Common Evaluation Methodology |
| CMS | Conversational Monitor System |
| CP | Control Program |
| CPACF | CP Assist for Cryptographic Functions |
| CPU | Central Processing Unit |
| DAC | Discretionary Access Control |
| DASD | Direct Access Storage Device |
| DPCM | Decreto del Presidente del Consiglio dei Ministri |
| DVD | Digital Versatile Disk |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| I/O | Input/Output |
| ID | Identifier |
| IT | Information Technology |
| LGP | Linea Guida Provvisoria |
| LGR | Live Guest Relocation |
| LPAR | Logical Partition |
| LVS | Laboratorio per la Valutazione della Sicurezza |
| MFA | Multi-factor Authentication |
| NIAP | National Information Assurance Partnership |
| NIS | Nota Informativa dello Schema |

| | |
|---------------|---|
| OCSI | Organismo di Certificazione della Sicurezza Informatica |
| PP | Protection Profile |
| PR/SM | Processor Resource/System Manager |
| PTF | Program Temporary Fix |
| RACF | Resource Access Control Facility |
| RNG | Random Number Generator |
| SAR | Security Assurance Requirement |
| SDF | Software Delivery and Fulfillment |
| SFR | Security Functional Requirement |
| SIE | Start Interpretive Execution |
| SSI | Single System Image |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSFI | TSF Interface |

4 References

4.1 Criteria and regulations

- [CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012
- [CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012
- [CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012
- [CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014
- [CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012
- [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 - Accredитamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004
- [LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004
- [NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013
- [NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013
- [NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

4.2 Technical documents

- [CR] “Certification Report IBM z/VM Version 7 Release 2”, OCSI/CERT/ATS/05/2020/RC, version 1.0, 30 April 2021

- [ETR] Final Evaluation Technical Report “IBM z/VM Version 7 Release 2”, OCSI-CERT-ATS-04-2021_ETR_220607_v2, Version 2, atsec information security GmbH, 7 June 2022

- [PP-VIRT] Protection Profile for Virtualization, pp_base_virtualization_v1.0, NIAP, Version 1.0, 17 November 2016

- [PP-EPSV] Protection Profile for Virtualization Extended Package Server Virtualization, ep_sv_v1.0, NIAP, Version 1.0, 17 November 2016

- [ST] “IBM z/VM Version 7 Release 2 for VPP Security Target”, Version 1.0, IBM Corporation, 16 May 2022

- [ZVM-CPG] z/VM V7.2 Certified Product Guidance, IBM Corporation

- [ZVM-SCG] z/VM V7.2 Secure Configuration Guide, SC24-6323-03, IBM Corporation, 12 May 2022

5 Recognition of the certificate

5.1 International recognition of CC certificates (CCRA)

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

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

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

This certificate is recognised under CCRA for all declared assurance components selected from CC Part 3 [CC3].

6 Statement of certification

The Target of Evaluation (TOE) is the product “IBM z/VM Version 7 Release 2 for VPP”, also referred to in the following as z/VM V7R2 or z/VM, developed by International Business Machines Corp. (IBM).

The TOE is a virtual machine hypervisor for IBM Z mainframe 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]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OC SI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

This Certification Report was issued at the conclusion of the re-certification of the same TOE (IBM z/VM Version 7 Release 2), already certified by OC SI (Certificate no. 2/21 of April 30, 2021 [CR]).

At the request of the Developer IBM Corp., the TOE was re-certified to meet the requirements of NIAP’s Protection Profile for Virtualization v1.0 [PP-VIRT], and the Server Virtualization Extended Package v1.0 [PP-EPSV]. The LVS atsec information security GmbH was able to reuse part of the documentation and evidences already provided in the previous evaluation.

While the considerations and recommendations already expressed for the previous TOE remain largely valid, for ease of reading this Certification Report has been rewritten in its entirety so as to constitute an autonomous document associated with the new TOE “IBM z/VM Version 7 Release 2 for VPP”.

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

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

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

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “IBM z/VM Version 7 Release 2 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 review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

| | |
|-----------------------------------|---|
| TOE name | IBM z/VM Version 7 Release 2 for VPP |
| Security Target | “IBM z/VM Version 7 Release 2 for VPP Security Target”, Version 1.0 [ST] |
| Evaluation Assurance Level | Conformant to PP including the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.1, 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, and AVA_VAN.1 |
| Developer | IBM Corporation |
| Sponsor | IBM Corporation |
| LVS | atsec information security GmbH |
| CC version | 3.1 Rev. 4 |
| PP conformance claim | Protection Profile for Virtualization v1.0 [PP-VIRT] with the following Extended Package: <ul style="list-style-type: none"> Protection Profile for Virtualization Extended Package Server Virtualization v1.0 [PP-EPSV] |
| Evaluation starting date | 21 June 2021 |
| Evaluation ending date | 7 June 2022 |

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.

7.3 Evaluated product

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

The TOE is z/VM Version 7 Release 2 clustered as up to four cooperating instances of z/VM within a Single System Image (SSI).

z/VM is a highly secure, flexible, robust, scalable operating system implementing a virtual machine hypervisor for IBM Z mainframe servers onto which to deploy mission-critical virtual servers. z/VM is 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. Apart from virtual servers, the TOE provides additional virtual machines for each logged in human user, separating the execution domain of each virtual machine from others as defined in the virtual machine definitions stored in the system directory. In addition to the system directory, the RACF security server is employed to mediate access to resources and privileged functions.

The TOE offers multi-system clustering technology allowing between one and four z/VM instances in a Single System Image (SSI) cluster. The cluster configuration as well as the cluster status are kept in resources shared amongst the cluster members. 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 their operation. The cluster members 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.

The RACF database used for maintaining the security context of the TOE is shared between the SSI cluster members. All cluster members run a local instance of RACF for local auditing, which has access to the shared RACF database.

The concept of virtual machines representing users maintained by a single z/VM instance can be expanded to match a cluster topology. While a virtual machine configured as USER is limited to run on only one of any of the cluster members at the same time, multiconfiguration virtual machines configured as IDENTITY may run simultaneously on different cluster members and typically represent service machines.

z/VM provides identification and authentication of users, discretionary access control (DAC) 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.

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

7.3.1 TOE architecture

7.3.1.1 TOE General Overview

The TOE is the z/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 four 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 (LPAR) of IBM mainframe servers.

The LPARs themselves are not part of the TOE, but belong 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.

The z/VM Single System Image feature (SSI) enables up to four z/VM systems to be configured as members of an SSI cluster, sharing different resources.

Members of the SSI cluster can be on the same or separate hardware systems. SSI enables the members of the cluster to be managed as one system, which allows maintenance to be applied to each member of the cluster while avoiding an outage of the entire cluster. SSI also implements the concept of Live Guest Relocation (LGR) where a running Linux guest operating system can be relocated from one member in an SSI cluster to another without the need to completely stop the running Linux guest throughout the whole process.

All z/VM member instances of one SSI cluster share the RACF database, but they do not share the RACF audit disks. Each z/VM member instance must execute its own instance of RACF accessing the shared RACF database. The sharing of the RACF database is done by sharing the DASD (Direct Access Storage Device) volume keeping the RACF database between the different SSI z/VM member instances. Although sharing of the RACF database between z/VM and z/OS is technically feasible, it is explicitly excluded from this evaluation.

Different instances of the TOE may also share the RACF database. The sharing is implemented similarly to the sharing of the RACF database within the SSI cluster. However, depending on the use scenario, such sharing may not be advisable.

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 (TSF) 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.

7.3.1.2 Major structural components of the TOE

The TOE consists of up to four z/VM instances each defined by three major components, i.e. the z/VM Control Program (CP), the Security Manager RACF, and the TCP/IP component, with RACF and TCP/IP running within specific virtual machines maintained by CP.

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:** a single-user general-purpose operating system that is employed to run the RACF and TCP/IP applications. CMS does not provide any security functionality but implements a file system that can be used by applications running on top.
- **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. For TLS-encrypted communication, it interacts with the SSL server, which is seen as a subcomponent of the TCP/IP component rather than an additional part of the TOE. Both the TCP/IP server and the SSL server are not part of CP, but each run within a respective virtual machine maintained by CP.

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 services allowing the establishment of a cryptographically secured channel.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

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

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

For supporting identification and authentication, the TOE employs RACF managing resource profiles and user profiles. Multi Factor Authentication decisions may also be deferred to an external MFA-provider, if configured. Such MFA-decisions are subsequently enforced by the TOE.

- **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;
 - access authority specified in the resource profile.

- **Separation of virtual machines:** operating system failures that occur in virtual machines cannot affect the TOE running on the real processor. As any error is isolated to a virtual machine, only that virtual machine fails and can be restarted without affecting any processes running in other virtual machines. In particular, mission-critical virtual servers are not affected by failures of virtual machines associated with the human users logged in.
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 the Control Program that cannot be isolated to one of its maintained virtual machines result in its abnormal termination (“abnormal end” or short “abend”). 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 mechanism.
Audit records concerning TLS connections are generated by the TLS server and are gathered by privileged users with access to the SSLADMIN command. These audit records are protected from unauthorized modification or deletion by the DAC 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.
DASD 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 TOE’s security functions. 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.

- 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.

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 sect. 8.3 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims exact conformance to the following Protection Profile and Extended Package:

- Protection Profile for Virtualization, Version 1.0 [PP-VIRT]
- Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0 [PP-EPSV]

7.6 Functional and assurance requirements

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

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

Considering that the Security Target [ST] claims exact conformance to the Protection Profile for Virtualization [PP-VIRT] and the Server Virtualization Extended Package [PP-EPSV], all and only the SARs and SFRs from the PP and EP are included.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize 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 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]. Furthermore, all specific assurance activities required by the Protection Profile for Virtualization [PP-VIRT] and the Server Virtualization Extended Package [PP-EPSV] have been carried out.

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

The evaluation was completed on 7 June 2022 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 8 June 2022. 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; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS atsec information security GmbH and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that the TOE “IBM z/VM Version 7 Release 2 for VPP” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the level of assurance as defined by the SARs included in the PP [PP-VIRT], 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 level of assurance as defined by the SARs included in the PP [PP-VIRT].

| 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 |
| Stated security requirements | ASE_REQ.1 | 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 |
| <i>Timely Security Updates</i> | <i>ALC_TSU_EXT.1</i> | Pass |
| Tests | Class ATE | Pass |
| Independent testing - conformance | ATE_IND.1 | Pass |
| Vulnerability assessment | Class AVA | Pass |

| Assurance classes and components | | Verdict |
|----------------------------------|-----------|---------|
| Vulnerability survey | AVA_VAN.1 | Pass |

Table 1 - Final verdicts for assurance requirements

8.2 Additional assurance activities

The Protection Profile for Virtualization [PP-VIRT] and the Server Virtualization Extended Package [PP-EPSV] include additional assurance activities that are specific to the TOE technology type, and are required for exact conformance to the PP and EP.

The Evaluators used for the PP/EP 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/EP are met.

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

| PP/EP assurance activities | Verdict | |
|--|------------|------|
| ASE: Security Target evaluation | ASE_BVPP.1 | Pass |
| | ASE_SVEP.1 | Pass |
| AGD: Guidance documents | AGD_BVPP.1 | Pass |
| | AGD_SVEP.1 | Pass |
| ALC: Life cycle support | ALC_BVPP.1 | Pass |
| ATE: Tests | ATE_BVPP.1 | Pass |
| | ATE_SVEP.1 | Pass |

Table 2 - Final verdicts for PP/EP assurance activities

8.3 Recommendations

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

Potential customers of the product “IBM z/VM Version 7 Release 2 for VPP” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions described in sect. 3.2 of the Security Target [ST] are respected.

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, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([ZVM-CPG], [ZVM-SCG]).

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

The TOE is software only, so no hardware or firmware is delivered as part of the product.

Table 3 contains the items that comprise the different elements of the TOE, including software and guidance.

| # | Type | Identifier | Release | Form of delivery |
|----------------------------|------|---|--------------|--------------------|
| z/VM Version 7 Release 2.0 | | | | |
| 1 | SW | z/VM Version 7 Release 2, program number 5741-A09 | V7R2 | DVD/ Electronic |
| 2 | DOC | Program Directory for z/VM V7R2 Base | GI13-4358-01 | Hard copy |
| 3 | DOC | Program Directory for RACF function level 720 | GI13-4364-01 | Hard copy |
| 4 | DOC | Guide for Automated Installation and Service | GC24-6292-02 | Hard copy |
| 5 | DOC | z/VM V7.2 Certified Product Guidance <u>sha256-Checksum:</u> 923da02dad4aa9bbc6c4a19ed565eac364f53914496578c0332c464078b56504 2022 May Refresh zVM720 Collection.zip | n/a | Soft copy |
| 6 | DOC | z/VM V7.2 Secure Configuration Guide for VPP <u>sha256-Checksum:</u> 21d55f6060b6f81b029143a2ddc203858906b1fadc6f42ccc91d1e78c764cfef hcps0_v7r2.pdf | SC24-6323-03 | Soft copy |
| Additional Media | | | | |
| 7 | SW | RSU1 (the z/VM 7.2 GA level of service) to be obtained electronically from IBM Shopz | n/a | Electronic |
| 8 | SW | PTF for APAR PH24751 to be obtained electronically from IBM Shopz | n/a | Electronic |
| 9 | SW | PTF for APAR VM66540 to be obtained electronically from IBM Shopz | n/a | Electronic |
| 10 | SW | PTF for APAR PH28216 to be obtained electronically from IBM Shopz | n/a | Electronic |

Table 3 - TOE Deliverables

Customers with proper IBM customer ID may use the IBM Shopz web portal (https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss) to file an order for the TOE. 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.

Orders for z/VM are processed by an SDF Production Center. The z/VM image ordered is duplicated to an appropriate DVD media set, which is then packed in a card-box and shrink wrapped. The final package is then delivered to the customer via a courier service together with a contents list.

The whole process starting at the preparation and labelling of the media until finally delivering the shrink-wrapped package to the customer is under supervision of a control system making use of bar code identification for all parts of an order throughout the complete process. The bar code enables unambiguous association of the media and the additional documentation to a specific order number and, hence, to the customer who filed that respective order.

Once the package arrived at the customer's site, the customer is able to verify that the delivery matches their order by reviewing the contents list provided as part of the delivery and by cross checking the part numbers labelled on the delivered media.

9.2 Identification of the TOE

During the order process for the TOE, the customer needs to explicitly order the CC-certified version of z/VM Version 7 Release 2. 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 [ZVM-SCG] 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 2.0, service level 2001 (64-bit)
```

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

```
VMFSIM QUERY 7VMCPR20 SRVAPPS * TDATA :PTF
VMFSIM QUERY 7VMRAC20 SRVAPPS * TDATA :PTF
VMFSIM QUERY 7VMTCP20 SRVAPPS * TDATA :PTF
```

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

For CP, the following PTFs should be reported:

```
UM35699
UMRSU01
```

For TCP/IP, the following PTF should be reported:

```
UI72767
UI72963
```

For RACF, no PTFs should be reported.

9.3 Installation, initialization and secure usage of the TOE

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

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- z/VM V7.2 Secure Configuration Guide [ZVM-SCG]
- z/VM V7.2 Certified Product Guidance [ZVM-CPG]

The Secure Configuration Guide contains references to other relevant guidance documentation contained in the z/VM 7.2 Certified Product Guidance. Both the Secure Configuration Guide and the Certified Product Guidance are available directly from a secured IBM ResourceLink:

<https://www.ibm.com/servers/resourceLink/svc0302a.nsf/pages/zVMV7R2Library>

and from the IBM z/VM 7.2 library accessible from:

<https://www.vm.ibm.com/library/index.html>

by following the respective hyperlink.

10 Annex B – Evaluated configuration

The Target of Evaluation is “IBM z/VM Version 7 Release 2 for VPP”, 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 is defined by an SSI cluster of up to four cooperating instances of the z/VM product each running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over that abstract machine regardless which software runs inside of virtual machines. The abstract machines are provided by a certified version of PR/SM on the following IBM z System processor, as indicated in sect. 1.5.4.4 of the Security Target [ST]:

- IBM Z z14 with CPACF Enablement Feature 3863 active

The LPARs themselves are not part of the TOE, but belong to the TOE environment. It is to be noted that although a z/VM instance technically can be run within a z/VM instance, the evaluated configuration is restricted to z/VM instances 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.

The evaluated configuration of the TOE is additionally defined by the configuration requirements to be met as stated in the Secure Configuration Guide [ZVM-SCG], which is part of the TOE deliverables.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level defined by the SARs included in the Protection Profile for Virtualization [PP-VIRT], such activities do not require the execution of functional tests by the Developer, but only independent functional tests and penetration tests by the Evaluators.

11.1 Test configuration

The independent Evaluator testing was performed on the same configuration, i.e. on systems GDLMCCC and GDLPCCC each running within a logical partition.

The logical partitions were provided by certified versions of PR/SM on a z14 (GDLPCCC) and a z15 (GDLMCCC) server, which - considering the fact that in an SSI cluster all members are restricted to a common CPU feature level, i.e. z14 in this case - is consistent with the supported hardware platform stated in section 1.5.4.4 of the Security Target [ST].

The test systems - for both the Developer and the Evaluators test sessions - had installed the TOE in its evaluated configuration as required by the Security Target [ST]. This was confirmed by the Evaluators analyzing Developer evidence generated and running respective checks on his own when setting up and running his independent tests.

11.2 Functional and independent tests performed by the Evaluators

Two types of tests were performed by the Evaluators: independent testing as defined in the Protection Profile for Virtualization [PP-VIRT] and the Server Virtualization Extended Package [PP-EPSV], and CAVS algorithm testing.

The Evaluators performed all the tests defined in the PP [PP-VIRT] and EP [PP-EPSV], which are around 100 tests. For the test requirements on crypto primitives and RNG, the CAVS tests were performed on all applicable cryptographic algorithms. The Evaluators tests are partly manual tests, and partly automated.

The independent testing mainly comprised of tests of the external interfaces, but there were also tests that target TOE security behavior that is normally hidden from the outside:

- communication modification: proxy setups were deployed in order to modify live-traffic to exercise the TOE behavior for situations where the TLS protocol is violated.

Multiple algorithm testing is required to be performed by the PP [PP-VIRT] and EP [PP-EPSV]. The CAVS cryptographic validation tool was used to verify the cryptographic interfaces with the given test vectors for validation.

All Evaluator test cases, including CAVS tests, were completed successfully, i.e., all the actual test results were consistent to the expected test results.

11.3 Vulnerability analysis and penetration tests

The Evaluator consulted public domain information in order to identify vulnerabilities that would require performing penetration testing, but found no such vulnerabilities.

As for the penetration testing based on the Evaluators' independent vulnerability analysis the Evaluators devised a total of two penetration test cases. Whereas one of the test cases was intended to identify additional interfaces potentially bearing weaknesses, the second test case was intended to explicitly probe for weaknesses of the TELNET server interface. All tests were performed at the depth of the subsystems of the TOE design exercising the TCP/IP subsystem of the TOE.

A port-scan was performed from within the same network segment the TOE was located in to eliminate interferences with other active network components. The tool *nmap* was used for that purpose. The tool identified no open ports on the TOE other than the TELNET ports, which was expected to be open for the purpose of establishing connections to the TOE as designed, thus matching the expected results.

Attempts to deliberately provoke buffer overflows during input of user credentials were performed. That test was performed using the standard clients to be used when accessing the TOE as well as from the command line. In particular, no specific setup reflecting other active network components was done. The tests revealed no weaknesses. The excessive inputs were rejected with error messages, thus matching the expected results.

The TLS implementation of the TOE was subject to protocol fuzzing using a publicly available test suite. The tests revealed no implementation errors or erratic behaviour of 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.