Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

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. 3/18

(Certification No.)

Prodotto: **IBM z/VM Version 6 Release 4**
(Product)

Sviluppato da: **IBM Corporation**
(Developed by)

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

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

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Rita Forsi)
Rita Forsi

Roma, 23 aprile 2018

Common Criteria

Fino a EAL2 *(Up to EAL2)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM z/VM Version 6 Release 4

OCSI/CERT/ATS/04/2017/RC

Version 1.0

23 April 2018

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	23/04/2018

2 Table of contents

3 Acronyms

APAR	Authorized Program Analysis Report
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CMS	Conversational Monitor System
CP	Control Program
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
I/O	Input/Output
ID	Identifier
IPL	Initial Program Load
IUCV	Inter User Communication Vehicle
IT	Information Technology
LGP	Linea Guida Provvisoria
LGR	Live Guest Relocation
LPAR	Logical Partition
LVS	Laboratorio per la Valutazione della Sicurezza
MAC	Mandatory Access Control
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
RSU	Recommended Service Upgrade
SAK	System Assurance Kernel
SAR	Security Assurance Requirement
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

[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

[ETR] Final Evaluation Technical Report “IBM z/VM Version 6 Release 4”, OCSI-CERT-ATS-04-2017_ETR_180313_v1, Version 1, atsec information security GmbH, 13 March 2018

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

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

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

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

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

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

[OSPP] Operating System Protection Profile, Version 2.0, BSI-CC-PP-0067, 01 June 2010

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

[OSPP-VIRT] OSPP Extended Package – Virtualization, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[ST] IBM z/VM Version 6 Release 4 Security Target, Version 1.2, IBM Corporation, 29 November 2017

[ZVM-CPG] z/VM V6.4 Certified Product Guidance, IBM Corporation

[ZVM-SCG] z/VM Version 6 Release 4 Secure Configuration Guide, Version SC24-6230-06, IBM Corporation, October 2017

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 http://www.commoncriteriaportal.org.

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

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “IBM z/VM Version 6 Release 4”, developed by International Business Machines Corp. (IBM).

z/VM Version 6 Release 4 (also referred to in the following as z/VM V6R4 or z/VM) is a virtual machine hypervisor for IBM z System mainframe 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 (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 v 3.1 for the assurance level EAL4, augmented with ALC_FLR.3, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

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

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "IBM z/VM Version 6 Release 4" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

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

7.2 Executive summary

TOE name	IBM z/VM Version 6 Release 4
Security Target	IBM z/VM Version 6 Release 4 Security Target, Version 1.2 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security GmbH
CC version	3.1 Rev. 5
PP conformance claim	Operating System Protection Profile v2.0 [OSPP] with the following Extended Packages (EP): • OSPP EP – Labeled Security v2.0 [OSPP-LS] • OSPP EP – Virtualization v2.0 [OSPP-VIRT]
Evaluation starting date	27 June 2017
Evaluation ending date	13 March 2018

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

7.3 Evaluated product

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

The TOE is z/VM Version 6 Release 4 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 System 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 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.

In its evaluated configuration, the TOE allows two modes of operation: a standard mode and a mode called Labeled Security Mode. In both modes of operation, the same software elements are used. The two modes have different RACF settings with respect to the use of security labels. All other configuration parameters are identical in the two modes.

The RACF database used for maintaining the security context of the TOE is shared between the 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.

The TOE 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.

TOE’s security functions are described more in detail in sect. 7.3.2.3.

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 sect. 1.5.4 of the Security Target [ST]. The TOE does not include hardware or firmware components.

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.

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 a logical partition (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.

In its evaluated configuration, the TOE allows two modes of operation: a standard mode meeting all requirements of the Operating System Protection Profile base [OSPP] and its extended package for Virtualization [OSPP-VIRT], and a more restrictive mode called Labeled Security Mode, which additionally meets all requirements of the OSPP extended package for Labeled Security [OSPP-LS]. In both modes of operation, the same software elements are used. The two modes have different RACF settings with respect to the use of security labels. All other configuration parameters are identical in the two modes.

7.3.1.2 Major software 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.

For a more detailed description of the TOE, please refer to sect. 1.5 (“TOE description”) of the z/VM V6R4 Security Target [ST].

7.3.2 TOE security features

7.3.2.1 Security policy

The security policy enforced is defined by the selected set of Security Functional Requirements (SFRs) and implemented by the TOE. It covers the following security aspects:

- Identification and Authentication
- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC) and Support for Security Labels
- Separation of virtual machines
- Auditing
- Object Reuse
- Security Management
- TSF Protection
- SSI clustering

7.3.2.2 Operational environment security objectives

The Assumptions defined in the Security Target [ST] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE operational environment. The following topics are of relevance:

- TOE administrators are competent and trustworthy.
- Remote trusted IT systems are sufficiently protected.
- TOE sensitive data are protected in an appropriate manner.
- TOE components are distributed, installed and configured in a secure manner.
- Product diagnostics are invoked at every scheduled maintenance period.
- TOE critical parts are protected from physical attacks.
- TOE is able to recover without a security compromise from a system failure or other discontinuity.
- Remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.

For a complete description of the security objectives for the TOE operational environment, please refer to sect. 4.2 of the z/VM V6R4 Security Target [ST].

7.3.2.3 Security functions

The TOE security functionality is described in detail in sect. 1.5.3 of the Security Target [ST]. The primary security features of the product that have been subject to evaluation are:

- **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
  - 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.

- **Mandatory Access Control (MAC) and Support for Security Labels**: In addition to DAC, the TOE provides Mandatory Access Control (MAC), which imposes access restrictions to information based on security classification. Each user and each RACF controlled object can have a security classification specified in its profile. The security classification can be a security level and zero or more security categories. Security labels are maintained separately from privilege classes in RACF.
  The access control enforced by the TOE ensures that users may only read labeled information if their security label dominates the information's label, and that they may only write to labeled information containers if the container's label dominates the subject's.

- **Separation of virtual machines**: Operating system failures that occur in virtual machines cannot affect the TOE running on the real processor. As the error is isolated to a virtual machine, only that virtual machine fails, and the user can re-IPL 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 one of its virtual machines maintained 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.

- **Auditing**: 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 the 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 MAC attributes is performed by security administrators in Labeled Security Mode.

  - 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.

- **SSI clustering**: The SSI clustering mechanism integrates different z/VM systems into one cluster in order to share different resources. The SSI cluster communication ensures serialization of concurrent access to shared resources, if needed.
  One of the main goals of SSI is the support of live guest relocation of virtual machines. The CP ensures the transfer of the virtual machine memory and state to another SSI cluster member without significant interruption of service of the virtual machine being relocated.

7.4 Documentation

The guidance documentation specified in Annex A - Guidelines for secure usage of the TOE is delivered to the customer together with the product. The guidance documentation contains all the information for installation, 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 sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims strict conformance to the following Protection Profiles and PP Packages:

- [OSPP] Operating System Protection Profile, Version 2.0, BSI-CC-PP-0067, 01 June 2010

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

7.6 Functional and assurance requirements

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

All Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2]. In particular, considering that the Security Target claims strict conformance to the [OSPP] PP, the following extended components from such PP are included:

- FDP_RIP.3: Full residual information protection of subjects
- FIA_USB.2: Enhanced user-subject binding.

Please refer to the Security Target [ST] for a 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].

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 13 March 2018 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 30 March 2018. Then, the Certification Body issued this Certification Report.

7.8 General considerations on the validity of the certification

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration.

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

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

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [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 TOE “IBM z/VM Version 6 Release 4” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

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

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

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

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

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

Potential customers of the product “IBM z/VM Version 6 Release 4” are suggested to properly understand the specific purpose of the certification reading this Certification Report together with the Security Target [ST].

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

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

It is assumed that the TOE can be operated in a secure manner only if the assumptions for the operational environment described in sect. 3.2 of the Security Target [ST] are respected. In particular, it is assumed that TOE administrators are adequately trained in the correct use of the TOE and selected among the trusted staff of the organization. The TOE is not designed to counter threats from inexperienced, malicious or negligent administrators.

It should also be noted that TOE security is conditioned by the proper functioning of the hardware platforms on which the TOE is installed, and of all trusted external IT systems supporting the implementation of TOE’s security policy. Specifications for the operational environment are described in the Security Target [ST].

9 Annex A - Guidelines for secure usage of the TOE

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

9.1 TOE delivery

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

Customers with proper IBM customer ID may use the IBM ShopzSeries web portal (https://www.ibm.com/software/shopzseries) to file an order of the TOE or may contact an IBM sales representative for support.

During the order process for the TOE, the customer needs to explicitly order the CC-certified version of z/VM Version 6 Release 4. This ensures that the product delivered to the customer actually is the TOE containing all required components.

As part of the order process, customers need to select the media they want the TOE to be delivered on and may choose between “Internet” and “DVD”. A selection of “Internet” will result in the TOE being downloaded from the SSL-secured website, while selection of “DVD” will trigger the production of a DVD media set.

Table 2 lists TOE materials that are delivered to the customer.

#	Type	Identifier	Release	Form of delivery
1	software	z/VM Version 6 Release 4, program number 5741-A07	V6R4	DVD/electronic
2	docs	Program Directory for z/VM V6R4 Base	GI13-3472-00	hard copy
3	docs	Program Directory for RACF function level 640	GI13-3478-03	hard copy
4	docs	Guide for Automated Installation and Service	GC24-6246-04	hard copy
5	docs	z/VM V6.4 Certified Product Guidance	n/a	soft copy
6	docs	z/VM V6R4 Secure Configuration Guide	SC24-6230-06	soft copy
7	software	PTF for APAR VM66077 containing RSU1 (the z/VM 6.4 GA level of service)	n/a	electronic

Table 2 - TOE deliverables

Orders for z/VM on DVD are processed by a 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 labeling 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 labeled on the delivered media.

9.2 Identification of the TOE

After installation of the product according to the Secure Configuration Guide [ZVM-SCG], the administrator is able to verify the version of the TOE by issuing the command:

```
QUERY CPLEVEL
```

which will result in displaying the version string Status:

```
z/VM Version 6 Release 4.0, service level 1601 (64bit)
```

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 6VMCPR40 SVRAPPS * TDATA :PTF
VMFSIM QUERY 6VMRAC40 SVRAPPS * TDATA :PTF
VMFSIM QUERY 6VMTCP40 SVRAPPS * 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:

```
UM34924 UM34897 UM34896 UM34895 UM34893
UM34890 UM34888 UM34887 UM34886 UMRSU02
```

For TCP/IP, no PTFs should be reported.

For RACF, no PTFs should be reported.

9.3 Installation, initialization and secure usage of the TOE

TOE installation and configuration 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 information for the secure initialization of the TOE and the preparation of its operational environment in accordance with the security objectives specified in the Security Target [ST]:

- z/VM Version 6 Release 4 Secure Configuration Guide [ZVM-SCG]
- z/VM V6.4 Certified Product Guidance [ZVM-CPG]

10 Annex B – Evaluated configuration

The Target of Evaluation is z/VM Version 6 Release 4. The TOE is software only and is accompanied by guidance documentation. The items listed in Table 2 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.

In the evaluated configuration of the TOE, each individual z/VM system in an SSI cluster is executed on an abstract machine provided by an LPAR on one of the supported hardware models of the IBM mainframe server families listed in section 1.5.4.4 of the Security Target [ST].

All those hardware models have in common the z/Architecture and the ability to be connected to various I/O devices but are different with respect to the number of the available central processors, which has been confirmed as not having any impact on the functionality of the TOE.

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]. The Security Target [ST] in section 1.5.4.3 redirects readers to this document, which is part of the TOE deliverables.

11 Annex C –Test activities

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

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

11.1 Test configuration

Developer testing as well as the independent Evaluators testing was performed on the same configuration, i.e. on the two test systems named GDLMCCC and GDLPCCC configured as SSI cluster members each running within a logical partition.

The logical partitions were provided by certified versions of PR/SM on two IBM zEC12 servers, which is consistent with the list of supported hardware platforms 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. 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.

Both test systems had installed the z/VM Version 6 Release 4 with SSI feature enabled, which was displayed as “z/VM Version 6 Release 4.0, Service Level 1601 (64-bit)” after logon. An analysis of the system installations performed by the Evaluators demonstrated that all required RSU and PTFs as stated in section 1.5.4.1 of the Security Target were installed on the machines.

The TOE had been in its evaluated configuration when the Developer tests were performed.

The limitation of tests performed to the test systems identified above was accepted, because the system configuration was considered to be representative for all allowed configurations. The TOE relies on an underlying abstract machine that is compliant with the z/Architecture definition. Extensive testing of the underlying hardware was performed by IBM on all processor configurations (including the chosen one) to verify full z/Architecture compliance of the abstract machine provided to the TOE.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer designed a specific CC related test suite that contains various test scenarios covering the security functions provided by the TOE.

The tests performed by the Developer directly stimulate the following TSFI identified in the Functional Specification and observe the resulting behaviour:

- CP commands
- RACF commands
- API
- RACF Report Writer
- TELNET Server

The following TSFI are tested indirectly by the tests performed and the required test setup:

- System Directory
- System Configuration
- TCP/IP configuration files and commands
- IUCV

All but two test cases are automated, i.e. after executing a script file, a significant amount of single tests are executed mediated by the CHUG test tool as well as the FACT test tool, the results of which are documented. Proper verification whether the actual test results match the expected results is already included in the respective test cases. The manual test cases related to the RACF Report Writer and the certificate based authentication implemented by the SSL Server contain sufficiently detailed information for the tester to decide on whether the actual test results obtained match the expected results.

IBM usually performs a significant amount of SAK testing verifying that the interface provided towards the virtual machines managed by the TOE is compliant with the z/Architecture definition. Those SAK tests, however, are to be considered negative tests, since they cannot actually prove compliance with z/Architecture but due to extensively issuing random processor instruction streams over a significant amount of time without ending up in any system errors, sufficient confidence of proper z/Architecture implementation is built up. Note that for the current evaluation no SAK tests at the level of z/VM were deemed necessary by the Developer as there have not been any changes to the z/Architecture since the previous evaluation. However, SAK tests have been actually performed at the level of the underlying PR/SM for the hardware platforms supported by z/VM and did not reveal any deviations as verified as part of the respective PR/SM evaluations performed.

11.2.2 Test coverage

The Developer testing was performed to the depth of the TOE design at subsystem level, i.e. the Developer test-depth analysis demonstrated that the TOE subsystems CP, RACF, and TCP/IP have been subject to test cases exercising the TSFI and the TSF implemented by those components.

11.2.3 Test results

The test evidence provided by the Developer and examined by the Evaluators demonstrates that all but one test case were successful, i.e. the TOE behaviour observed during the tests matched the expected behaviour.

For test cases related to one specific TSFI, deviations from the expected behaviour were identified, which resulted in opening a respective bugfix record. A profound analysis of the error performed by the Developer resulted in the determination that the observed deviations do not present a security/integrity issue, i.e. no security mechanisms of the TOE were bypassed or disabled and no vulnerability is introduced.

The Evaluators were able to verify that corrective actions to address the failure have been initiated already. According to the Developer they will be effective in the next release of the product.

The Certification Body (OCSI) recommends that this flaw be fixed by the Developer before applying for a re-evaluation of the TOE.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators repeated a randomly chosen subset of the Developer tests. For each of the test case groups “CP commands” (including 100% of SSI and SSL tests performed), “RACF commands”, and “DIAGNOSE”, coverage of at least 42% was achieved by the sampling strategy. The overall coverage achieved by the sample chosen was 46%.

No SAK tests were repeated.

In addition, the Evaluators devised independent test cases to cover the TSFI that are not explicitly but only implicitly triggered by the Developer tests repeated. The independent Evaluators test cases directly trigger the TELNET Server, the TCP/IP configuration files and commands, the System Directory, and RACF and CP commands. The Evaluators covered all TSFI except the API comprising the z/Architecture instructions and the RACF Report Writer by independent test cases, with those not explicitly listed above being triggered indirectly.

11.3.2 Test coverage

By using Developer tests as base for independent testing, the Evaluators achieved the same test depth as the Developer when repeating a subset of the Developer tests. Therefore, the tests performed by the Evaluators were at the level of the subsystems of the TOE design.

11.3.3 Test results

All but one Developer tests re-performed passed, i.e. the actual results achieved by the Evaluators matched the expected results. For the failing test case, the Developer provided a rationale on why the test returned a result that deviated from the expected output.

Corrective actions to properly address the issue, which is not considered critical, have been already initiated but not yet completed.

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

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

11.4 Vulnerability analysis and penetration tests

11.4.1 Testing approach

The Evaluators 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 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.

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 port, 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 TOE is not vulnerable to the Robot attack, as determined by the test program provided by the publishers of the attack.

11.4.2 Test coverage

All tests were performed at the depth of the subsystems of the TOE design exercising the TCP/IP subsystem of the TOE.

11.4.3 Test results

The independent search for vulnerabilities performed by the Evaluators did not reveal any vulnerabilities that are exploitable in the intended operational environment of the TOE by attackers with an assumed attack potential of at most Enhanced-Basic.

11.4.4 Residual vulnerabilities

The following vulnerabilities, potentially affecting all kinds of operating systems, have been discovered and addressed by the Developer and confirmed by the Evaluators as being residual:

- vulnerability to various types of malware (trojan horses, viruses, worms);
- vulnerability to buffer overflows;
- vulnerability to hardware architecture design flaws.

Exploitation of the above vulnerabilities requires an attack potential that goes beyond the assumed attack potential of Enhanced-Basic. In particular, the attack potential required to develop proper exploits for buffer overflows and architectural attacks has been calculated as Beyond High.